

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Xiaomang ZHANG, Teruaki MORITA, Conf: Unknown  
Masayuki EHIRO

Application No.: New Application Group: Unknown

Filed: August 1, 2003 Examiner: Unknown

For: **ELECTRONIC SEAL, IC CARD, AUTHENTICATION SYSTEM  
USING THE SAME, AND MOBILE DEVICE INCLUDING SUCH  
ELECTRONIC SEAL**

**PRIORITY LETTER**

August 1, 2003

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sirs:

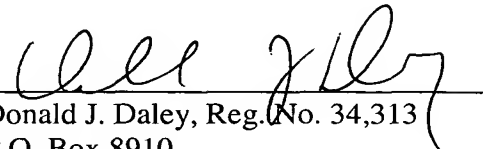
Pursuant to the provisions of 35 U.S.C. 119, enclosed is/are a certified copy of the following priority document(s).

<u>Application No.</u>	<u>Date Filed</u>	<u>Country</u>
2002-225590	8/2/2002	JAPAN

In support of Applicant's priority claim, please enter this document into the file.

Respectfully submitted,

HARNESS, DICKY, & PIERCE, P.L.C.

By   
Donald J. Daley, Reg. No. 34,313  
P.O. Box 8910  
Reston, Virginia 20195  
(703) 668-8000

DJD:me

(Translation)

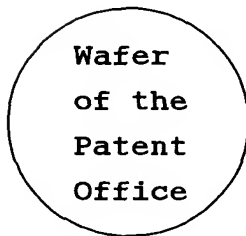
PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following  
application as filed with this Office.

Date of Application : August 2, 2002

Application Number : Patent Appln. No. 2002-225590

Applicant(s) : SHARP KABUSHIKI KAISHA



June 12, 2003

Shinichiro OTA  
  
Commissioner,  
Patent Office

Seal of  
Commissioner  
of  
the Patent  
Office

Appln. Cert. No.

Appln. Cert. Pat. 2003-3046039

日 本 国 特 許 庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 8月 2日

出 願 番 号

Application Number:

特願2002-225590

[ ST.10/C ]:

[ JP2002-225590 ]

出 願 人

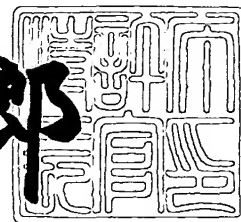
Applicant(s):

シャープ株式会社

2003年 6月12日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3046039

【書類名】 特許願

【整理番号】 02J01269

【提出日】 平成14年 8月 2日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00  
G07D 7/00

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内

【氏名】 張 小▲忙▼

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内

【氏名】 森田 晃明

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内

【氏名】 永廣 雅之

【特許出願人】

【識別番号】 000005049

【氏名又は名称】 シャープ株式会社

【代理人】

【識別番号】 100078282

【弁理士】

【氏名又は名称】 山本 秀策

【選任した代理人】

【識別番号】 100062409

【弁理士】

【氏名又は名称】 安村 高明

【選任した代理人】

【識別番号】 100107489

【弁理士】

【氏名又は名称】 大塩 竹志

【手数料の表示】

【予納台帳番号】 001878

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0208587

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子印鑑、ＩＣカード、本人認証システムおよび携帯機器

【特許請求の範囲】

【請求項１】 所定鍵に基づいて暗号化された乱数値を入力する入力手段と

、  
該所定鍵と関連した秘密鍵を記憶する秘密鍵記憶手段と、

該秘密鍵記憶手段の秘密鍵に基づいて、該入力手段によって入力された乱数値を復号する復号手段と、

該秘密鍵記憶手段の秘密鍵に基づいて、該復号手段によって復号化された乱数値を暗号化する暗号化手段と、

該暗号化手段によって暗号化された乱数値を出力する出力手段とを備えた電子印鑑。

【請求項２】 前記入力手段は、所定鍵に基づいて暗号化された返信要求ＩＤ（Identification）を入力すると、前記復号手段は、秘密鍵に基づいて、入力した返信要求ＩＤを復号化し、

返信要求ＩＤを記憶する返信要求ＩＤ記憶手段と、

該返信要求ＩＤ記憶手段に記憶された返信要求ＩＤと該復号手段によって復号化された返信要求ＩＤとを比較する比較手段とを更に備え、

前記暗号化手段は、該比較手段による比較結果が一致した場合に、該秘密鍵に基づいて、該復号手段で復号化した乱数値を暗号化する請求項１記載の電子印鑑

。【請求項３】 前記秘密鍵記憶手段は、各カード会社ＩＤ番号毎に秘密鍵が記憶されており、カード会社ＩＤ番号が前記入力手段によって入力されると、入力されたカード会社ＩＤ番号に基づいて該秘密鍵が特定される請求項１または２記載の電子印鑑。

【請求項４】 乱数値を発生する乱数値発生手段と、

所定鍵を記憶する所定鍵記憶手段と、

該所定鍵に基づいて、該乱数値発生手段によって発生させた乱数値を暗号化する暗号化手段と、

該暗号化手段によって暗号化された乱数値を出力する出力手段と、

所定鍵と関連した秘密鍵に基づいて暗号化された乱数値を入力する入力手段と

該所定鍵に基づいて、該入力手段によって入力された乱数値を復号する復号手段と、

該乱数値発生手段によって発生させた乱数値と該復号手段によって復号化された乱数値とを比較する比較手段とを備えた I C カード。

【請求項 5】 返信要求 I D を記憶する返信要求 I D 記憶手段をさらに備え

前記暗号化手段は、前記所定鍵に基づいて、該返信要求 I D 記憶手段に記憶した返信要求 I D を暗号化し、前記出力手段は、暗号化された返信要求 I D を出力する請求項 4 記載の I C カード。

【請求項 6】 各カード会社毎のカード会社 I D 番号を記憶するカード会社 I D 番号記憶手段をさらに備え、

該カード会社 I D 番号を前記出力手段により出力する請求項 4 または 5 記載の I C カード。

【請求項 7】 前記所定鍵記憶手段は、各カード会社 I D 番号毎に所定鍵が記憶されている請求項 4 記載の I C カード。

【請求項 8】 請求項 4 ～ 7 のいずれかに記載の I C カードと、

請求項 1 ～ 3 のいずれかに記載の電子印鑑とを備え、該 I C カードと電子印鑑とが互いにデータ交換することにより本人認証処理を行う本人認証システム。

【請求項 9】 前記 I C カードの乱数値発生手段で発生させた乱数値が所定鍵に基づいて暗号化されて前記電子印鑑に出力され、該電子印鑑によって入力された乱数値が秘密鍵に基づいて復号化され、復号化された乱数値が秘密鍵に基づいて暗号化されて該 I C カードに出力され、該 I C カードによって入力された乱数値が所定鍵に基づいて復号化され、復号化された乱数値と該乱数値発生手段によって発生させた元の乱数値とが一致した場合のみ本人であると認証するようにした請求項 8 記載の本人認証システム。

【請求項 1 0】 所定鍵に基づいて暗号化された乱数値を入力する入力手段

と、

該所定鍵と関連した秘密鍵を記憶する秘密鍵記憶手段と、

該秘密鍵記憶手段の秘密鍵に基づいて、該入力手段によって入力された乱数値を復号する復号手段と、

利用者の固有情報を記憶する利用者固有情報記憶手段と、

該復号手段によって復号化された乱数値と該利用者の固有情報とを用いてハッシュ演算を行ったハッシュ演算値を出力するハッシュ演算手段と、

該秘密鍵記憶手段の秘密鍵に基づいて、該ハッシュ演算値を暗号化する暗号化手段と、

該暗号化手段によって暗号化されたハッシュ演算値を出力する出力手段とを備えた電子印鑑。

【請求項 1 1】 前記入力手段は、所定鍵に基づいて暗号化された返信要求 I D を入力すると、前記復号手段は、秘密鍵に基づいて、入力した返信要求 I D を復号化し、

返信要求 I D を記憶する返信要求 I D 記憶手段と、

該返信要求 I D 記憶手段に記憶された返信要求 I D と該復号手段によって復号化された返信要求 I D とを比較する比較手段とを更に備え、

前記暗号化手段は、該比較手段による比較結果が一致した場合に、該秘密鍵に基づいて、前記ハッシュ演算値を暗号化する請求項 1 0 記載の電子印鑑。

【請求項 1 2】 前記秘密鍵記憶手段は、各カード会社 I D 番号毎に秘密鍵が記憶されており、カード会社 I D 番号が前記入力手段によって入力されると、入力されたカード会社 I D 番号に基づいて秘密鍵が特定される請求項 1 0 または 1 1 記載の電子印鑑。

【請求項 1 3】 乱数値を発生する乱数値発生手段と、

所定鍵を記憶する所定鍵記憶手段と、

該所定鍵に基づいて、該乱数値発生手段で発生させた乱数値を暗号化する暗号化手段と、

該暗号化手段によって暗号化された乱数値を出力する出力手段と、

利用者の固有情報を記憶する利用者固有情報記憶手段と、



該乱数値発生手段によって発生させた乱数値と該利用者の固有情報とを用いてハッシュ演算を行ったハッシュ演算値を出力するハッシュ演算手段と、

該所定鍵と関連した秘密鍵に基づいて暗号化されたハッシュ演算値を入力する入力手段と、

該入力手段によって入力されたハッシュ演算値を該所定鍵に基づいて復号する復号手段と、

該ハッシュ演算手段から出力されたハッシュ演算値と該復号手段によって復号化されたハッシュ演算値とを比較する比較手段とを備えたＩＣカード。

【請求項１４】 前記比較手段による比較結果が一致した場合に本人であると認証し、核比較結果が不一致の場合に本人ではないと認証する本人認証手段を更に備えた請求項４または１３記載のＩＣカード。

【請求項１５】 返信要求ＩＤを記憶する返信要求ＩＤ記憶手段をさらに備え、

前記暗号化手段は、前記所定鍵に基づいて、前記返信要求ＩＤ記憶手段に記憶された返信要求ＩＤを暗号化し、前記出力手段は、暗号化された返信要求ＩＤを出力する請求項１３記載のＩＣカード。

【請求項１６】 各カード会社毎のカード会社ＩＤ番号を記憶するカード会社ＩＤ番号記憶手段をさらに備え、

前記出力手段は、該カード会社ＩＤ番号を出力する請求項１３または１５記載のＩＣカード。

【請求項１７】 前記所定鍵記憶手段は、各カード会社ＩＤ番号毎に所定鍵が記憶されている請求項１６記載のＩＣカード。

【請求項１８】 請求項１３～１７のいずれかに記載のＩＣカードと、  
請求項１０～１２のいずれかに記載の電子印鑑とを備え、該ＩＣカードと電子印鑑とが互いにデータ交換することにより本人認証処理を行う本人認証システム。

【請求項１９】 前記ＩＣカードの乱数値発生手段で発生させた乱数値が所定鍵に基づいて暗号化されて前記電子印鑑に出力されると共に該乱数値発生手段で発生させた元の乱数値と利用者の固有情報とが前記ハッシュ演算手段によって

ハッシュ演算され、該電子印鑑に入力された乱数値が秘密鍵に基づいて復号化され、復号化された乱数値と利用者の固有情報とがハッシュ演算されたハッシュ演算値が該ＩＣカードに対して出力され、該ＩＣカードに入力されたハッシュ演算が所定鍵に基づいて復号化され、該ハッシュ演算手段から出力されたハッシュ演算値と該復号手段で復号化されたハッシュ演算値とが一致した場合のみ本人であると認証するようにした請求項１８記載の本人認証システム。

【請求項２０】 前記所定鍵は公開鍵であり、前記秘密鍵は該公開鍵と所定の関数を介して鍵ペアを構成する請求項１～３および１０～１２のいずれかに記載の電子印鑑。

【請求項２１】 前記所定鍵は公開鍵であり、前記秘密鍵は該公開鍵と所定の関数を介して鍵ペアを構成する請求項４～７および１３～１７のいずれかに記載のＩＣカード。

【請求項２２】 請求項１～３、１０～１２および２０のいずれかに記載の電子印鑑が収納された携帯機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えば市役所の窓口業務や電子商取引などに用いられ、本人認証を行うために用いられる電子印鑑、ＩＣカードおよびそれらを用いた本人認証システム、この電子印鑑を収納した携帯機器に関する。

【０００２】

【従来の技術】

従来から、市役所の窓口、商取引などにおいて、本人認証は印鑑（伝統印鑑）の捺印によって行われている。印鑑は、盗難などに遭った場合に気づき易いため、早急に被害防止対策を講じることができる。

【０００３】

また、近年では、ＩＣカード、電子商取引、暗号化Ｅメールなどのように、情報が電子データ化（デジタルデータ化）されて流通されるようになってきており、それに伴って、本人認証の方法についても変化してきている。

【 0 0 0 4 】

ＩＣカード、ＩＤカード、電子商取引、暗号化Ｅメールなどにおいて、セキュリティ機能としては非常に強固なものが要求されるが、そのセキュリティ機能は、例えば４桁の暗証番号などのように、非常に脆弱な手段によって守られている。

【 0 0 0 5 】

例えば、電子財布として利用されるＩＣカード（Ｓｍａｒｔ Ｃａｒｄとも称される）には、クレジットカードとキャッシュカードとがあり、クレジットカードの場合にはＩＣカードによるセキュリティチェックと筆記署名の目視確認という二つの要素で本人認証が行われ、キャッシュカードの場合にはＩＣカードによるセキュリティチェックと暗証番号の入力確認という二つの要素で本人認証が行われる。

【 0 0 0 6 】

しかしながら、模倣署名を目視判断で見破ることは容易ではなく、暗号番号は４桁の数字であるために安全性が低い。さらに安全性を高めるために、暗証データの桁数を増やすと、利用者の記憶に負担を強いることになる。

【 0 0 0 7 】

ＩＣカードの安全性を高めるためには、署名、指紋、声紋、網膜パターン、顔などといった利用者固有の情報に基づいて本人認証を行う方法が考えられるが、そのアルゴリズムなどのソフト面や装置などのハード面からユーザ操作手数などの運営面までを考えると、それをＩＣカードが利用される現場で応用することは容易ではない。

【 0 0 0 8 】

また、ＩＣカードは、主として欧米において、携帯電話器、ケーブルテレビジョン装置などの課金に対しても利用されており、そのセキュリティチェックは利用者に提供されるＰＩＮナンバーによって行われている。このため、上記暗証番号と同様に、安全性の面で問題がある。

【 0 0 0 9 】

また、入退室管理カードのようなＩＤカードは広く用いられているが、ＩＤカ

ードによって確認するだけで本人と認められることが多い。しかしながら、このような I D カードは、紛失・盗難などによって、簡単に悪用され得る。

#### 【 0 0 1 0 】

また、電子商取引における安全性は、認証局によって証明書が発行された専用 W e b ブラウザに依存している。その専用 W e b ブラウザを利用するためには暗証番号が必要であるが、その暗証番号が漏れると、ブラウザ内部のセキュリティは強固であっても、誰でもアクセスすることができるようになる。

#### 【 0 0 1 1 】

暗号化 E メールについては、暗号化関連の鍵などが計算機によって管理されているため、その計算機を利用する人であれば、自由に暗号化メールを読み書きすることができる。

#### 【 0 0 1 2 】

図 1 0 は、従来の本人認証システムの一例を示すブロック図である。

#### 【 0 0 1 3 】

図 1 0 において、この本人認証システム 1 1 0 は、カード関連内容のバックアップをしている遠隔サーバ 1 1 1 と、例えば相関情報、セキュリティ処理情報および暗証番号照合情報などが記憶された I C カード 1 1 2 と、サービス内容表示処理、選択実行処理、セキュリティ処理および暗証番号入力処理などの各種処理を行うホストコンピュータ 1 1 3 と、I C カード 1 1 2 とホストコンピュータ 1 1 3 の交信インターフェイスおよび、非接触カードへの電源供給を行うとカードリーダー/カードライター 1 1 4 とを備え、I C カードをキャッシュカードとして用いる場合に本人認証を行う。

#### 【 0 0 1 4 】

遠隔サーバ 1 1 1 には、I C カード 1 1 2 に関する情報がバックアップ保存されているが、遠隔サーバ 1 1 1 にアクセスするためにはリアルタイム通信が必要であるため、本人認証は、I C カード 1 1 2 とホストコンピュータ 1 1 3 の間および、ユーザとホストコンピュータ 1 1 3 の間で行われる。

#### 【 0 0 1 5 】

I C カード 1 1 2 およびホストコンピュータ 1 1 3 はセキュリティ機能を有し

ており、ＩＣカード１１２が接触型である場合には、インターフェイスとしてのカードリーダー／カードライター１１４を介してＩＣカード１１２とホストコンピュータ１１３との間で互いにセキュリティチェックのためにデータ通信が行われる。

【 0 0 1 6 】

また、ＩＣカード１１２が非接触型である場合には、カードリーダー／カードライター１１４からＩＣカード１１２に対して電源が供給され、ホストコンピュータ１１３とＩＣカード１１２との間で互いにセキュリティチェックのためにデータ通信が行われる。

【 0 0 1 7 】

そのセキュリティチェックにおいて、ホストコンピュータ１１３がそのＩＣカード１１２を真性であると確認すると、ホストコンピュータ１１３のディスプレイに暗証番号入力画面が表示される。

【 0 0 1 8 】

次に、ユーザによって暗証番号が入力装置１１５から入力されると、入力された暗証番号がホストコンピュータ１１３からカードリーダー／カードライター１１４を介してＩＣカード１１２に供給され、ＩＣカード１１２の内部で暗証番号の照合が行われる。この暗証番号の照合結果によって本人と確認されると、ＩＣカード１１２の使用が認められる。ユーザによってサービス内容が選択されると、ホストコンピュータ１１３によってそのサービスが実行されて、ホストコンピュータ１１３のディスプレイにサービス内容が表示される。

【 0 0 1 9 】

【発明が解決しようとする課題】

前述したように、ＩＣカードやＩＤカードなどでは、カード自体の真偽判断が重視されており、署名（サイン）、暗証番号などを補助的に利用して本人認証を行っている。また、本人認証におけるセキュリティのレベルは、カードの用途によって異なっており、低いセキュリティレベルでは、カードによる認証だけで本人として認められることがある。署名については模倣することができ、暗号番号については４桁程度の数字が利用されていることから、現在よりもカードのセキ

ユリティレベルを高める必要がある。

【 0 0 2 0 】

しかしながら、暗証データ桁数の増加、署名、指紋、声紋、網膜パターンおよび顔などといった利用者固有の情報を利用して安全性を高める方法は、利用者の習慣、手数および技術などの面で実現が容易ではない。

【 0 0 2 1 】

また、電子商取引、暗号化 E メールなどにおいても、Web ブラウザ自身の真偽判断が重視されているため、同様の問題が生じている。

【 0 0 2 2 】

本発明は、上記従来の問題を解決するもので、ユーザに負担をかけることなく、本人認証の安全性を更に高めることができる電子印鑑、IC カードおよびそれらを用いた本人認証システム、この電子印鑑を収納した携帯機器を提供することを目的とする。

【 0 0 2 3 】

【課題を解決するための手段】

本発明の電子印鑑は、所定鍵に基づいて暗号化された乱数値を入力する入力手段と、所定鍵と関連した秘密鍵を記憶する秘密鍵記憶手段と、秘密鍵記憶手段の秘密鍵に基づいて、入力手段によって入力された乱数値を復号する復号手段と、秘密鍵記憶手段の秘密鍵に基づいて、復号手段によって復号化された乱数値を暗号化する暗号化手段と、暗号化手段によって暗号化された乱数値を出力する出力手段とを備えており、そのことにより上記目的が達成される。

【 0 0 2 4 】

また、好ましくは、本発明の電子印鑑における入力手段は、所定鍵に基づいて暗号化された返信要求 ID (Identification) を入力すると、復号手段は、秘密鍵に基づいて、入力した返信要求 ID を復号化し、

返信要求 ID を記憶する返信要求 ID 記憶手段と、返信要求 ID 記憶手段に記憶された返信要求 ID と復号手段によって復号化された返信要求 ID とを比較する比較手段とを更に備え、

暗号化手段は、該比較手段による比較結果が一致した場合に、該秘密鍵に基づ

いて、該復号手段で復号化した乱数値を暗号化する。

【 0 0 2 5 】

さらに、好ましくは、本発明の電子印鑑における秘密鍵記憶手段は、各カード会社 I D 番号毎に秘密鍵が記憶されており、カード会社 I D 番号が前記入力手段によって入力されると、入力されたカード会社 I D 番号に基づいて秘密鍵が特定される。

【 0 0 2 6 】

本発明の I C カードは、乱数値を発生する乱数値発生手段と、所定鍵を記憶する所定鍵記憶手段と、所定鍵に基づいて、乱数値発生手段によって発生させた乱数値を暗号化する暗号化手段と、暗号化手段によって暗号化された乱数値を出力する出力手段と、所定鍵と関連した秘密鍵に基づいて暗号化された乱数値を入力する入力手段と、所定鍵に基づいて、入力手段によって入力された乱数値を復号する復号手段と、乱数値発生手段によって発生させた乱数値と復号手段によって復号化された乱数値とを比較する比較手段とを備えており、そのことにより上記目的が達成される。

【 0 0 2 7 】

また、好ましくは、本発明の I C カードにおける返信要求 I D を記憶する返信要求 I D 記憶手段をさらに備え、暗号化手段は、所定鍵に基づいて、返信要求 I D 記憶手段に記憶した返信要求 I D を暗号化し、出力手段は、暗号化された返信要求 I D を出力する。

【 0 0 2 8 】

さらに、好ましくは、本発明の I C カードにおいて、各カード会社毎のカード会社 I D 番号を記憶するカード会社 I D 番号記憶手段をさらに備え、カード会社 I D 番号を前記出力手段により出力する。

【 0 0 2 9 】

さらに、好ましくは、本発明の I C カードにおける所定鍵記憶手段は、各カード会社 I D 番号毎に所定鍵が記憶されている。

【 0 0 3 0 】

本発明の本人認証システムは、請求項 4 ～ 7 のいずれかに記載の I C カードと

、請求項 1 ～ 3 のいずれかに記載の電子印鑑とを備え、ＩＣカードと電子印鑑とが互いにデータ交換（交信）することにより本人認証処理を行っており、そのことにより上記目的が達成される。

【 0 0 3 1 】

また、好ましくは、本発明の本人認証システムにおいて、ＩＣカードの乱数値発生手段で発生させた乱数値が所定鍵に基づいて暗号化されて電子印鑑に出力され、電子印鑑によって入力された乱数値が秘密鍵に基づいて復号化され、復号化された乱数値が秘密鍵に基づいて暗号化されてＩＣカードに出力され、ＩＣカードによって入力された乱数値が所定鍵に基づいて復号化され、復号化された乱数値と乱数値発生手段によって発生させた元の乱数値とが一致した場合のみ本人であると認証する。

【 0 0 3 2 】

本発明の電子印鑑は、所定鍵に基づいて暗号化された乱数値を入力する入力手段と、所定鍵と関連した秘密鍵を記憶する秘密鍵記憶手段と、秘密鍵記憶手段の秘密鍵に基づいて、入力手段によって入力された乱数値を復号する復号手段と、利用者の固有情報を記憶する利用者固有情報記憶手段と、復号手段によって復号化された乱数値と利用者の固有情報とを用いてハッシュ演算を行ったハッシュ演算値を出力するハッシュ演算手段と、秘密鍵記憶手段の秘密鍵に基づいて、ハッシュ演算値を暗号化する暗号化手段と、暗号化手段によって暗号化されたハッシュ演算値を出力する出力手段とを備えており、そのことにより上記目的が達成される。

【 0 0 3 3 】

また、好ましくは、本発明の電子印鑑における入力手段は、所定鍵に基づいて暗号化された返信要求ＩＤを入力すると、復号手段は、秘密鍵に基づいて、入力した返信要求ＩＤを復号化し、

返信要求ＩＤを記憶する返信要求ＩＤ記憶手段と、返信要求ＩＤ記憶手段に記憶された返信要求ＩＤと復号手段によって復号化された返信要求ＩＤとを比較する比較手段とを更に備え、

暗号化手段は、比較手段による比較結果が一致した場合に、秘密鍵に基づいて



、ハッシュ演算値を暗号化する。

【 0 0 3 4 】

さらに、好ましくは、本発明の電子印鑑における秘密鍵記憶手段は、各カード会社 I D 番号毎に秘密鍵が記憶されており、カード会社 I D 番号が入力手段によって入力されると、入力されたカード会社 I D 番号に基づいて秘密鍵が特定される。

【 0 0 3 5 】

本発明の I C カードは、乱数値を発生する乱数値発生手段と、所定鍵を記憶する所定鍵記憶手段と、所定鍵に基づいて、乱数値発生手段で発生させた乱数値を暗号化する暗号化手段と、暗号化手段によって暗号化された乱数値を出力する出力手段と、利用者の固有情報を記憶する利用者固有情報記憶手段と、乱数値発生手段によって発生させた乱数値と利用者の固有情報とを用いてハッシュ演算を行ったハッシュ演算値を出力するハッシュ演算手段と、所定鍵と関連した秘密鍵に基づいて暗号化されたハッシュ演算値を入力する入力手段と、入力手段によって入力されたハッシュ演算値を所定鍵に基づいて復号する復号手段と、ハッシュ演算手段から出力されたハッシュ演算値と該復号手段によって復号化されたハッシュ演算値とを比較する比較手段とを備えており、そのことにより上記目的が達成される。

【 0 0 3 6 】

また、好ましくは、本発明の I C カードにおいて、比較手段による比較結果が一致した場合に本人であると認証し、この比較結果が不一致の場合に本人ではないと認証する本人認証手段を更に備える。

【 0 0 3 7 】

さらに、好ましくは、本発明の I C カードにおいて、返信要求 I D を記憶する返信要求 I D 記憶手段をさらに備え、暗号化手段は、所定鍵に基づいて、返信要求 I D 記憶手段に記憶された返信要求 I D を暗号化し、出力手段は、暗号化された返信要求 I D を出力する。

【 0 0 3 8 】

さらに、好ましくは、本発明の I C カードにおいて、各カード会社毎のカード

会社 I D 番号を記憶するカード会社 I D 番号記憶手段をさらに備え、出力手段は、カード会社 I D 番号を出力する。

## 【 0 0 3 9 】

さらに、好ましくは、本発明の I C カードにおける所定鍵記憶手段は、各カード会社 I D 番号毎に所定鍵が記憶されている。

## 【 0 0 4 0 】

本発明の本人認証システムは、請求項 1 3 ～ 1 7 のいずれかに記載の I C カードと、請求項 1 0 ～ 1 2 のいずれかに記載の電子印鑑とを備え、この I C カードと電子印鑑とが互いにデータ交換することにより本人認証処理を行っており、そのことにより上記目的が達成される。

## 【 0 0 4 1 】

また、好ましくは、本発明の本人認証システムにおいて、I C カードの乱数値発生手段で発生させた乱数値が所定鍵に基づいて暗号化されて電子印鑑に出力されると共に乱数値発生手段で発生させた元の乱数値と利用者の固有情報とがハッシュ演算手段によってハッシュ演算され、電子印鑑に入力された乱数値が秘密鍵に基づいて復号化され、復号化された乱数値と利用者の固有情報とがハッシュ演算されたハッシュ演算値が I C カードに対して出力され、I C カードに入力されたハッシュ演算が所定鍵に基づいて復号化され、ハッシュ演算手段から出力されたハッシュ演算値と該復号手段で復号化されたハッシュ演算値とが一致した場合のみ本人であると認証する。

## 【 0 0 4 2 】

また、好ましくは、本発明の電子印鑑における所定鍵は公開鍵であり、秘密鍵は公開鍵と所定の関数を介して鍵ペアを構成する。また同様に、好ましくは、本発明の I C カードにおける所定鍵は公開鍵であり、秘密鍵は公開鍵と所定の関数を介して鍵ペアを構成する。この所定鍵は公開鍵および秘密鍵を含んでいる。

## 【 0 0 4 3 】

本発明の電子機器は、請求項 1 ～ 3、1 0 ～ 1 2 および 2 0 のいずれかに記載の電子印鑑が収納されており、そのことにより上記目的が達成される。

## 【 0 0 4 4 】

上記構成により、以下、本発明の作用について説明する。

【 0 0 4 5 】

本発明においては、ＩＣカードなどを用いたデジタル時代の本人認証に対応するために、秘密鍵に基づいて暗号化・復号化を行う電子印鑑を導入することによって、ユーザに負担をかけることなく、本人認証の安全性が向上する。

【 0 0 4 6 】

この秘密鍵は、電子印鑑に閉じ込められており、暗号化技術を用いて本人認証のためのデータを送受信することにより、秘密鍵を外部からアクセスされないようにすることができ、秘密鍵が盗難されることを防いで、本人認証の安全性を向上させることができる。また、電子印鑑による本人認証は、ＩＣカードを用いて暗証番号により本人認証を行う場合のように、桁数が多い暗証番号を利用者が記憶する必要がないため、利用者に負担をかけることはない。

【 0 0 4 7 】

例えば、所定鍵としての公開鍵に基づいて暗号化・復号化を行うＩＣカードと、所定鍵と関連した鍵ペアの秘密鍵に基づいて暗号化・復号化を行う電子印鑑とを組み合わせることによって、公開鍵方式暗号技術によって本人認証を行うことができる。

【 0 0 4 8 】

まず、ＩＣカードの乱数値発生手段によって発生された乱数値を公開鍵に基づいて暗号化して電子印鑑に対して送信する。電子印鑑によって受信した乱数値を秘密鍵に基づいて復号化し、復号化された乱数値を秘密鍵に基づいて暗号化してＩＣカードに対して送信する。ＩＣカードによって受信した乱数値を公開鍵に基づいて復号化し、復号化された乱数値と乱数値発生手段によって発生させた元の乱数値とが一致した場合に、本人であると確認することができる。

【 0 0 4 9 】

また、ＩＣカードから公開鍵に基づいて暗号化した乱数値を電子印鑑に対して送信する際に、公開鍵に基づいて暗号化された返信要求ＩＤを共に送信する。電子印鑑によって受信した返信要求ＩＤを秘密鍵に基づいて復号化し、復号化された乱数値と、返信要求ＩＤ記憶手段に記憶された返信要求ＩＤとが一致した場合

に、復号化された乱数値を秘密鍵に基づいて暗号化してＩＣカードに対して送信する。一致しない場合には、処理を終了する。これによって、さらに本人認証の安全性を向上させることができる。

#### 【 0 0 5 0 】

この公開鍵は、カード会社などに広く利用してもらうことができる。また、電子印鑑は、カード会社ＩＤ番号毎に秘密鍵を記憶しておくことによって、カード会社ＩＤ番号から秘密鍵を特定して用いることもできる。なお、本発明の電子印鑑は、公開鍵方式暗号技術の他、秘密鍵方式暗号技術を用いて本人認証を行うこともできる。

#### 【 0 0 5 1 】

さらに、利用者の署名、指紋、声紋、網膜パターン、顔写真など、利用者固有の情報を電子データ化して、暗号化技術を用いてデータを入出力（送受信；無線）して確認することより、より安全性を向上させることができる。

#### 【 0 0 5 2 】

電子印鑑は、指輪、ブレスレット、イヤリングなどのアクセサリ、眼鏡など、利用者が身に付けてあまり離さないような携帯機器に装着することによって、紛失しにくくすることができ、さらに安全性を向上させることができる。また、電子印鑑は、盗難などにより無くなった場合に気付きやすいため、無形の暗証番号に比べて被害防止対策を早急に行うことができる。

#### 【 0 0 5 3 】

##### 【発明の実施の形態】

以下に、本発明の本人認証システムの実施形態１，２について図面を参照しながら説明する。

##### （実施形態１）

図１は、本発明の本人認証システムの実施形態１における要部構成を示すブロック図である。

#### 【 0 0 5 4 】

図１において、この本人認証システム１００は、カード関連内容をバックアップ保持している遠隔サーバ１１と、例えば相関情報、セキュリティ、公開鍵によ

る暗号化および符号化機能を持つＩＣカード１２と、サービス内容表示処理、選択実行処理、セキュリティ処理、暗証番号入力処理などの各種処理を行うホストコンピュータ１３と、ＩＣカード１１２とホストコンピュータ１１３の通信インターフェイスであり、非接触カードへの電源供給を行うカードリーダー／カードライター１４と、秘密鍵による暗号化および符号化機能を持つ電子印鑑１６とを備えている。

## 【 0 0 5 5 】

遠隔サーバ１１には、カード関連内容が保存されているが、遠隔サーバ１１にアクセスするためにはリアルタイム通信が必要であるため、本人認証はＩＣカード１２および電子印鑑１６とホストコンピュータ１３との間で行われる。

## 【 0 0 5 6 】

ＩＣカード１２およびホストコンピュータ１３はセキュリティ機能を有しており、ＩＣカード１２が接触型である場合にも、インターフェイスとしてのカードリーダー／カードライター１４を介してホストコンピュータ１３とＩＣカード１２との間で互いにセキュリティチェックのためにデータ通信が行われる。また、ＩＣカード１２が非接触型である場合には、カードリーダー／カードライター１４からＩＣカード１２に対して電源が供給され、ホストコンピュータ１３とＩＣカード１２との間でセキュリティチェックのために互いにデータ通信が行われる。

## 【 0 0 5 7 】

そのセキュリティチェックにおいて、ホストコンピュータ１３とＩＣカード１２との間で互いに真性であると確認されると、ＩＣカード１２および電子印鑑１６によって公開鍵方式暗号技術によって本人認証が行われる。詳細に後述するが、本人であることが確認されると、ＩＣカード１２の使用が認められ、ホストコンピュータ１３のディスプレイにサービス内容が表示される。ユーザによって入力装置１５からサービス内容が選択されると、ホストコンピュータ１３によってそのサービスが実行されるようになっている。

## 【 0 0 5 8 】

また、よりセキュリティを高めるために、以上に加えて、ホストコンピュータ１３のディスプレイに対して入力装置１５から暗証番号を入力して本人認証を行

うようにしてもよい。この場合には、入力された暗証番号がカードリーダー／カードライタ 1 4 を介して IC カード 1 2 に供給され、IC カード 1 2 の内部で暗証番号の照合が行われることになる。この暗証番号の照合結果によって本人と確認されると、IC カード 1 2 の使用が認められることになる。

## 【 0 0 5 9 】

電子印鑑 1 6 における秘密鍵は公開鍵と関連しており、公開鍵と所定の関数を介して鍵ペアを構成している。

## 【 0 0 6 0 】

即ち、詳細に後述する本人認証処理手順で使用される公開鍵  $K_p$  および秘密鍵  $K_s$  の鍵ペアは、例えば公開鍵暗号のアルゴリズムとして広く用いられている RSA 方式の場合には、以下のようにして決定される。

## 【 0 0 6 1 】

まず、二つの素数  $P$  および  $Q$  を選択する。ここで、素数とは、1 およびその数自身を除く他の数では割り切れない整数であり、例えば、2、3、5、7、11・・・である。

## 【 0 0 6 2 】

次に、公開鍵  $K_p$  に対応する値  $E$  を決定し、

$$(D \times E) \% N_1 = 1 \cdots (\text{式 } 1)$$

$$N_1 = (P - 1) \times (Q - 1)$$

によって秘密鍵  $K_s$  に対応する値  $D$  を求める。上記（式 1）の左辺は、 $(D \times E)$  を  $N_1$  で割ったときの余りの値であり、上記（式 1）の右辺の値 = 1 を満たすように、上記（式 1）の左辺から値  $D$  を求める。

## 【 0 0 6 3 】

これによって、公開鍵  $K_p = (E, N)$  および秘密鍵  $K_s = (D, N)$  が得られる。ここで、 $N = P \times Q$  によって求められる。

## 【 0 0 6 4 】

上記公開鍵  $K_p$  は、カード会社などのような関連組織に自由に利用してもらうことが便利である。一方、上記秘密鍵  $K_s$  は、電位印鑑 1 6 の中に閉じ込められており、アクセスできないようになっているため、安全性を向上させることがで

きる。

【 0 0 6 5 】

図 2 は、図 1 の I C カード 1 2 の内部構成を示すブロック図である。

【 0 0 6 6 】

図 2 において、この I C カード 1 2 は、アンテナ回路 2 0 1 と、整流回路 2 0 2 と、クロック抽出回路 2 0 3 と、復調回路 2 0 4 と、定電圧発生回路 2 0 5 と、パワーオンリセット回路 2 0 6 と、変調回路 2 0 7 と、本人認証手段を持つ内部ロジック回路 2 0 8 と、所定鍵記憶手段としての公開鍵記憶手段 2 0 9 と、返信要求 I D 記憶手段 2 1 0 と、乱数発生手段 2 1 1 と、ワークメモリ 2 1 2 と、暗号化手段 2 1 3 と、カード会社 I D 番号記憶手段 2 1 4 と、合成回路 2 1 5 と、復号手段 2 1 6 と、比較手段 2 1 7 とを備えている。これらのアンテナ回路 2 0 1、整流回路 2 0 2、クロック抽出回路 2 0 3 および復調回路 2 0 4 により入力手段（ここでは受信手段であるが、接触型の場合を含んでいる）が構成され、また、アンテナ回路 2 0 1、整流回路 2 0 2、変調回路 2 0 7 および内部ロジック回路 2 0 8 により出力手段（ここでは送信手段であるが、接触型の場合を含んでいる）が構成されている。

【 0 0 6 7 】

アンテナ回路 2 0 1 は送受信手段であり、カードリーダー／カードライター 1 4 からの信号が受信され得ると共に、I C カード 1 2 からの信号がカードリーダー／カードライター 1 4 に送信され得る。

【 0 0 6 8 】

整流回路 2 0 2 では、アンテナ回路 2 0 1 を介して受信された信号を整流してクロック抽出回路 2 0 3 および復調回路 2 0 4 に出力し、また、変調回路 2 0 7 からの信号を整流してアンテナ回路 2 0 1 に出力する。

【 0 0 6 9 】

クロック抽出回路 2 0 3 は、アンテナ回路 2 0 1 を介して受信されたカードリーダー／カードライター 1 4 からのキャリア波から動作に必要なクロック信号が抽出され、内部ロジック回路 2 0 8 に出力する。

【 0 0 7 0 】

復調回路 2 0 4 では、送受信手段であるアンテナ回路 2 0 1 を介して受信されたカードリーダー／カードライタ 1 4 からの信号が復調されて内部ロジック回路 2 0 8 に出力する。

【 0 0 7 1 】

定電圧発生回路 2 0 5 では、定電圧をパワーオンリセット回路 2 0 6 および内部ロジック回路 2 0 8 に出力する。

【 0 0 7 2 】

パワーオンリセット回路 2 0 6 は、I C カード 1 2 の電源遮断／リセットを制御する回路であり、内部ロジック回路 2 0 8 に電源遮断／リセットのための制御信号を出力する。

【 0 0 7 3 】

変調回路 2 0 7 では、内部ロジック回路 2 0 8 による制御に基づいて、所定のキャリア波が任意の波長に変調され、アンテナ回路 2 0 1 を介してカードリーダー／カードライタ 1 4 に送信される。

【 0 0 7 4 】

内部ロジック回路 2 0 8 は、C P U （中央演算処理装置）および、R O M および R A M からなるメモリなどを有しており、I C カード 1 2 を構成する各回路を制御する。また、内部ロジック回路 2 0 8 の本人認証手段は、比較手段 2 1 7 からの比較結果を受けて、その比較結果が一致した場合には本人であると判断し、その比較結果が一致しない場合には本人ではないと判断する。

【 0 0 7 5 】

なお、以上のアンテナ回路 2 0 1 ～変調回路 2 0 7 の構成は、カードリーダー／カードライタ 1 4 と I C カード 1 2 とが非接触型で交信する場合の一例を示したが、この構成に限定されるものではなく、カードリーダー／カードライタ 1 4 と I C カード 1 2 とが接触型で交信する場合として、図 2 の以外の構成を用いることも可能である。次の公開鍵記憶手段 2 0 9 ～比較手段 2 1 7 は接触型および非接触型で共通である。

【 0 0 7 6 】

公開鍵記憶手段 2 0 9 には各カード会社 I D 番号毎に所定鍵としての公開鍵 K



p がそれぞれ記憶されている。なお、ここでは、所定鍵として公開鍵  $K_p$  として  
いるが秘密鍵であってもよい。

【0077】

返信要求 ID 記憶手段 210 には返信要求 ID が記憶されている。

【0078】

乱数発生手段 211 では乱数  $D_1$  をランダムに発生する。

【0079】

ワークメモリ 212 には乱数発生手段 211 で発生させた乱数  $D_1$  を記憶する

【0080】

暗号化手段 213 では、ワークメモリ 212 に記憶された乱数  $D_1$  と、返信要  
求 ID 記憶手段 210 に記憶された返信要求 ID とを、各カード会社 ID 番号に  
対応した公開鍵  $K_p$  に基づいて暗号化する。

【0081】

カード会社 ID 番号記憶手段 214 には各カード会社毎にカード会社 ID 番号  
が記憶されている。

【0082】

合成回路 215 では、カード会社 ID 番号、暗号化された返信要求 ID および  
暗号化された乱数 ( $D_1$  を暗号化したもの) が合成され、その合成値が内部ロジ  
ック回路 208 から変調回路 207、整流回路 202 さらにアンテナ回路 201  
を経てカードリーダー/カードライター 14 に送信される。

【0083】

復号手段 216 では、カードリーダー/カードライター 14 から送信され、アンテ  
ナ回路 201 で受信された信号が、復調回路 204 から内部ロジック回路 208  
を経て供給された暗号化された乱数信号を、公開鍵  $K_p$  に基づいて乱数  $D_3$  に復  
号する。

【0084】

比較手段 217 では、復号手段 216 で復号化された乱数  $D_3$  と乱数発生手段  
211 で発生された乱数  $D_1$  とが比較され、その比較結果が内部ロジック回路 2

08に供給される。内部ロジック回路208において、前述したように、その比較結果が一致した場合に本人であると判断し、その比較結果が一致しない場合に本人ではないと判断する。

【0085】

図3は、図1の電子印鑑16の内部構成を示すブロック図である。

【0086】

図3において、この電子印鑑16は、アンテナ回路301と、整流回路302と、クロック抽出回路303と、復調回路304と、定電圧発生回路305と、パワーオンリセット回路306と、変調回路307と、内部ロジック回路308と、カード会社ID番号と他の情報データの分離手段309と、カード会社ID番号・秘密鍵記憶手段310と、復号手段311と、返信要求ID記憶手段312と、比較手段としての返信要求ID有無判断手段313と、暗号化手段314とを備えている。これらのアンテナ回路301、整流回路302、クロック抽出回路303および復調回路304により入力手段（ここでは受信手段であるが、接触型の場合を含んでいる）が構成され、また、アンテナ回路301、整流回路302、変調回路307および内部ロジック回路308により出力手段（ここでは送信手段であるが、接触型の場合を含んでいる）が構成されている。

【0087】

アンテナ回路301は、送受信手段であり、カードリーダー／カードライター14からの信号が受信されると共に、電子印鑑16からの信号がカードリーダー／カードライター14に送信される。

【0088】

整流回路302では、アンテナ回路301を介して受信された信号を整流して復調回路304およびクロック抽出回路303に出力され、また、変調回路307からの信号を整流してアンテナ回路301に出力される。

【0089】

クロック抽出回路303では、アンテナ回路301を介して受信されたカードリーダー／カードライター14からのキャリア波から動作に必要なクロック信号が抽出され、内部ロジック回路308に出力される。

## 【 0 0 9 0 】

復調回路 3 0 4 では、送受信手段であるアンテナ回路 3 0 1 を介して受信されたカードリーダー／カードライター 1 4 からの信号を復調して、内部ロジック回路 3 0 8 に出力する。

## 【 0 0 9 1 】

定電圧発生回路 3 0 5 では、定電圧をパワーオンリセット回路 3 0 6 および内部ロジック回路 3 0 8 に出力する。

## 【 0 0 9 2 】

パワーオンリセット回路 3 0 6 は、電子印鑑 1 6 の電源遮断／リセットを制御する回路であり、電源遮断／リセットのための制御信号を内部ロジック回路 3 0 8 に出力する。

## 【 0 0 9 3 】

変調回路 3 0 7 は、内部ロジック回路 3 0 8 からの制御に基づいて、所定のキャリア波を任意の波長に変調して、アンテナ回路 3 0 1 を介してカードリーダー／カードライター 1 4 側に送信される。

## 【 0 0 9 4 】

内部ロジック回路 3 0 8 は、CPU（中央演算処理装置）および、ROMおよびRAMからなるメモリなどを有しており、電子印鑑 1 6 を構成する各回路を制御する。

## 【 0 0 9 5 】

なお、以上のアンテナ回路 3 0 1 ～変調回路 3 0 7 の構成は、カードリーダー／カードライター 1 4 と電子印鑑 1 6 とが非接触型で交信する場合の一例を示したが、図 3 の構成に限定されるものではなく、例えばカードリーダー／カードライター 1 4 と電子印鑑 1 6 とが接触型で交信する場合には、図 3 の以外の構成を用いることも可能である。次のカード会社 ID 番号と他の情報データの分離手段 3 0 9 ～暗号化手段 3 1 4 は接触型および非接触型で共通である。

## 【 0 0 9 6 】

カード会社 ID 番号と他の情報データの分離手段 3 0 9 は、カードリーダー／カードライター 1 4 から送信されてアンテナ回路 3 0 1 で受信され、整流回路 3 0 2

から復調回路 3 0 4 さらに内部ロジック回路 3 0 8 を介して供給された信号を、カード会社 I D 番号と他の情報データ（公開鍵  $K_p$  に基づいて暗号化された返信要求 I D および暗号化された乱数）とに分離する。

## 【 0 0 9 7 】

カード会社 I D 番号・秘密鍵記憶手段 3 1 0 は、各カード会社 I D 番号毎に秘密鍵  $K_s$  がそれぞれ記憶されており、分離手段 3 0 9 からカード会社 I D 番号が供給されると、そのカード会社 I D 番号に対応した秘密鍵  $K_s$  が復号手段 3 1 1 に供給される。

## 【 0 0 9 8 】

復号手段 3 1 1 では、公開鍵  $K_p$  に基づいて暗号化された返信要求 I D および乱数とが分離手段 3 0 9 から供給され、カード会社 I D 番号・秘密鍵記憶手段 3 1 0 から供給された秘密鍵  $K_s$  に基づいて、その返信要求 I D および乱数とがそれぞれ復号化される。

## 【 0 0 9 9 】

返信要求 I D 記憶手段 3 1 2 には返信要求 I D が記憶されている。

## 【 0 1 0 0 】

返信要求 I D 有無判断手段 3 1 3 では、復号手段 3 1 1 によって復号化された返信要求 I D と、返信要求 I D 記憶手段 3 1 2 に記憶されている返信要求 I D とが比較されて、その比較結果が一致した場合には返信要求 I D が含まれていたと判断し、一致しない場合には返信要求 I D が含まれていなかったと判断して、その判定信号を暗号化手段 3 1 4 に出力する。

## 【 0 1 0 1 】

暗号化手段 3 1 4 は、判定信号の結果が「有」の場合（返信要求 I D が含まれていたと判断された場合）に、復号手段 3 1 1 によって復号化された乱数  $D_2$  を、カード会社 I D 番号・秘密鍵記憶手段 3 1 0 から出力された秘密鍵  $K_s$  に基づいて暗号化する。なお、判定信号の結果が「無」の場合（返信要求 I D が含まれていなかったと判断された場合）には、復号手段 3 1 1 によって復号化された乱数  $D_2$  は、暗号化手段 3 1 4 によって暗号化されず、処理を終了する。

## 【 0 1 0 2 】

なお、電子印鑑 1 6 は、携帯機器に収納されていることが望ましく、特に、紛失などを防ぐためには、利用者が常に身に付ける指輪、ブレスレット、イヤリングなどのようなアクセサリ、または眼鏡などに装着されていることが望ましい。

#### 【 0 1 0 3 】

図 4 は、図 1 のカードリーダー／カードライター 1 4 の内部構成を示すブロック図である。

#### 【 0 1 0 4 】

図 4 において、このカードリーダー／カードライター 1 4 は、変調回路 4 0 1 と、復調回路 4 0 2 と、アンテナ回路 4 0 3 と、不揮発性メモリ 4 0 4、信号処理装置 4 0 5、制御回路 4 0 6 と、入出力 I / F（インターフェイス）回路 4 0 7 とを備えている。

#### 【 0 1 0 5 】

変調回路 4 0 1 は、信号処理回路 4 0 5 からの信号が所定のキャリア波に変調されてアンテナ回路 4 0 3 に供給される。例えば 1 3 . 5 6 M H Z のキャリア波が A S K（Amplitude Shift Keying）方式でアンテナ回路 4 0 3 によって送信される。

#### 【 0 1 0 6 】

復調回路 4 0 2 は、アンテナ回路 4 0 3 からの所定のキャリア波が復調されて信号処理回路 4 0 5 に供給される。

#### 【 0 1 0 7 】

信号処理装置 4 0 5 は、制御回路 4 0 6 からの制御に基づいて、I C カード 1 2 および電子印鑑 1 6 からのデータ入出力が検出され、データ通信の際に送受信される信号が処理される。

#### 【 0 1 0 8 】

制御回路 4 0 6 は、内部に C P U（中央演算処理装置）およびメモリなどを有しており、不揮発性メモリ 4 0 4 に予め記録されている制御プログラムを読み込んでそれを起動させることにより、カードリーダー／カードライター 1 4 を構成する各回路部を制御すると共に、入出力 I / F 回路 4 0 7 を介して、ホストコンピュータ 1 3 などの上位装置とのデータ通信が行われる。

## 【 0 1 0 9 】

上記構成により、以下、本実施形態 1 の本人認証システム 1 0 0 において、公開鍵方式暗号技術を用いて本人認証を行う場合の処理手順について説明する。

## 【 0 1 1 0 】

図 5 は、図 1 の本人認証システム 1 0 0 を用いた本人認証処理手順を示すフローチャートである。なお、ここでは、処理する部分を明確にするために、ＩＣカード 1 2、カードリーダー／カードライター 1 4 および電子印鑑 1 6 のブロックを併せて記載している。

## 【 0 1 1 1 】

図 5 に示すように、まず、ステップ S 1 0 1 において、ＩＣカード 1 2 側では、乱数発生手段 2 1 1 によって、乱数 D 1 をランダムに生成する。

## 【 0 1 1 2 】

次に、ステップ S 1 0 2 では、暗号化手段 2 1 3 によって、生成された乱数 D 1 と返信要求 I D とを公開鍵 K p に基づいて暗号化する。カード会社の I D 番号と公開鍵 K p に基づいて暗号化された乱数 D 1 と公開鍵 K p に基づいて暗号化された返信要求 I D とを、カードリーダー／カードライター 1 4 を介して電子印鑑 1 6 に送信する。

## 【 0 1 1 3 】

さらに、ステップ S 1 0 3 において、電子印鑑 1 6 側では、受信されたカード会社の I D 番号から秘密鍵 K s を特定する。

## 【 0 1 1 4 】

ステップ S 1 0 4 では、公開鍵 K p に基づいて暗号化された乱数 D 1 と公開鍵 K p に基づいて暗号化された返信要求 I D とを、復号手段 3 1 1 によって、ステップ S 1 0 3 で特定された秘密鍵 K s に基づいて復号する。これによって、復号化された返信要求 I D と復号化された乱数 D 2 とが得られる。

## 【 0 1 1 5 】

さらに、ステップ S 1 0 5 では、復号化された返信要求 I D と返信要求 I D 記憶手段 3 1 4 に記憶されている返信要求 I D とを比較して、返信要求 I D が含まれているか否かを判断する。送信要求 I D が含まれていない場合（NO）には、

ステップ S 1 0 6 に進み、処理を終了する。一方、送信要求 I D が含まれている場合 (Y E S) には、ステップ S 1 0 7 の処理に進み、復号化した乱数 D 2 を、暗号化手段 3 1 3 によって、S 1 0 3 で特定された秘密鍵 K s に基づいて暗号化する。この暗号化された乱数 (D 2 を暗号化したもの) を I C カード 1 2 に送信する。

## 【 0 1 1 6 】

さらに、ステップ S 1 0 8 において、I C カード 1 2 側では、受信された、暗号化された乱数を、復号手段 2 1 6 によって公開鍵 K p に基づいて復号することによって乱数 D 3 を得る。

## 【 0 1 1 7 】

さらに、ステップ S 1 0 9 では、ステップ S 1 0 1 で生成された乱数 D 1 とステップ S 1 0 8 で得られた乱数 D 3 との照合を行う。この照合結果が一致した場合 (Y E S) には、ステップ S 1 1 0 の処理に進み、本人であると認める。

## 【 0 1 1 8 】

また、ステップ S 1 0 9 で照合結果が不一致であれば (N O) 、ステップ S 1 1 1 の処理に進み、本人として認めないという判断を下す。

## 【 0 1 1 9 】

なお、本人認証の際には、I C カード 1 2 によって生成される乱数の桁 (範囲) が長い方が、安全性を向上するためには好ましい。また、本人認証は、I C カード 1 2 側と電子印鑑 1 6 側との送受信を複数回行うようにしてもよい。但し、電子印鑑 1 6 側からの返信回数の合計がある閾値を超えると、秘密鍵が解読されて安全性が低くなる虞がある。よって、電子印鑑 1 6 の内部に、この返信回数の合計を記憶するカウンタを設けて、カウンタ C 1 の値が閾値を超えると、電子印鑑 1 6 の鍵を更新するなどの手段を講じることが望ましい。また、集中的に暗号解読が試みられて秘密鍵が漏れることを防ぐために、予め設定された短い期間 (1 回の認証処理に対する期間) 内での返信回数を記憶するカウンタを設けて、その期間内で返信回数が予め設定された最大回数を超えると、電子印鑑 1 6 からの返信を行わないようにすることが望ましい。

## 【 0 1 2 0 】

また、電子印鑑 1 6 の秘密鍵記憶手段 3 1 0 には、デフォルトの秘密鍵を記憶させることができるが、拡張用の記憶領域を設けることによって、カード会社は、自社の I D 番号およびその I D 番号に対応した秘密鍵を記憶させることができ、デフォルトの秘密鍵と自社鍵とを選択して用いることができる。

#### 【 0 1 2 1 】

さらに、上記説明では、公開鍵方式を利用して電子印鑑 1 6 と I C カード 1 2 との間で本人認証を行っているが、電子印鑑 1 6 は、公開鍵方式であっても秘密鍵方式であっても対応可能である。秘密鍵方式の場合には、電子印鑑 1 6 との間で本人認証のために交信を行う機器においても、秘密鍵による暗号化・復号化機能を設ければよい。

#### 【 0 1 2 2 】

また、上記説明では、キャッシュカードなどとして利用される I C カードのセキュリティ機能を向上するために本発明の電子印鑑を用いた例を説明しているが、これを用いて、上記と同様に、電子商取引、暗号化 E メールなどのセキュリティ機能を強化することもできる。

#### （実施形態 2）

本実施形態 2 では、上記実施形態 1 よりも更にセキュリティを向上させるために、上記 I C カード 1 2 および電子印鑑 1 6 に更に利用者固有情報を記憶させている場合である。

#### 【 0 1 2 3 】

図 6 は、本発明の本人認証システムの実施形態 2 における I C カードの内部構成を示すブロック図である。なお、図 2 の I C カードと同様の機能を有する部材には同じ符号を付してその説明を省略する。

#### 【 0 1 2 4 】

図 6 において、この I C カード 1 2 A は、アンテナ回路 2 0 1 と、整流回路 2 0 2 と、クロック抽出回路 2 0 3 と、復調回路 2 0 4 と、定電圧発生回路 2 0 5 と、パワーオンリセット回路 2 0 6 と、変調回路 2 0 7 と、内部ロジック回路 2 0 8 と、公開鍵記憶手段 2 0 9 と、返信要求 I D 記憶手段 2 1 0 と、乱数発生手段 2 1 1 と、ワークメモリ 2 1 2 と、暗号化手段 2 1 3 と、カード会社 I D 番号



記憶手段 2 1 4 と、合成回路 2 1 5 と、復号手段 2 1 6 A と、利用者固有情報記憶手段 2 1 8 と、ハッシュ演算手段 2 1 9 と、比較手段 2 1 7 A とを備えている。ここで、上記実施形態 1 の場合と異なるのは、復号手段 2 1 6 A、利用者固有情報記憶手段 2 1 8、ハッシュ演算手段 2 1 9 および比較手段 2 1 7 A である。

【 0 1 2 5 】

利用者固有情報記憶手段 2 1 8 には、利用者の固有情報が記憶されており、利用者の固有情報として、例えば、暗証番号、利用者の署名、指紋、声紋、網膜パターン、顔写真などが挙げられる。

【 0 1 2 6 】

ハッシュ演算手段 2 1 9 では、ワークメモリ 2 1 2 に記憶された乱数 D 1 と利用者固有情報記憶手段 2 1 8 に記憶された利用者の固有情報とから、ハッシュ演算が行われ、ハッシュ演算データ H 1 が生成される。

【 0 1 2 7 】

一方、復号手段 2 1 6 A では、カードリーダー／カードライター 1 4 から送信され、アンテナ回路 2 0 1、整流回路 2 0 2、復調回路 2 0 4 および内部ロジック回路 2 0 8 を介して供給された暗号化されたハッシュ演算データが公開鍵 K p 1 に基づいて復号化され、これによってハッシュ演算データ H 3 が得られる。

【 0 1 2 8 】

比較手段 2 1 7 A では、復号手段 2 1 6 A で復号化されたハッシュ演算データ H 3 とハッシュ演算手段 2 1 9 でハッシュ演算されたハッシュ演算データ H 1 とが比較され、その比較結果が内部ロジック回路 2 0 8 に供給される。

【 0 1 2 9 】

内部ロジック回路 2 0 8 では、その比較結果が一致した場合には本人であると判断し、比較結果が一致しない場合には、本人ではないと判断する。

【 0 1 3 0 】

図 7 は、本発明の本人認証システムの実施形態 2 における電子印鑑の内部構成を示すブロック図である。なお、図 3 の電子印鑑 1 6 と同様の機能を有する部材については同じ符号を付してその説明を省略する。

【 0 1 3 1 】

図 7 において、この電子印鑑 1 6 A は、アンテナ回路 3 0 1 と、整流回路 3 0 2 と、クロック抽出回路 3 0 3 と、復調回路 3 0 4 と、定電圧発生回路 3 0 5 と、パワーオンリセット回路 3 0 6 と、変調回路 3 0 7 と、内部ロジック回路 3 0 8 と、分離手段 3 0 9 と、カード会社 I D 番号・秘密鍵記憶手段 3 1 0 と、復号手段 3 1 1 と、返信要求 I D 記憶手段 3 1 2 と、比較手段としての返信要求 I D 有無判断手段 3 1 3 と、利用者固有情報記憶手段 3 1 4 と、ハッシュ演算手段 3 1 5 と、暗号化手段 3 1 6 とを備えている。ここで、上記実施形態 1 の場合と異なるのは、利用者固有情報記憶手段 3 1 4、ハッシュ演算手段 3 1 5 および暗号化手段 3 1 6 A である。

#### 【 0 1 3 2 】

利用者固有情報記憶手段 3 1 4 には、利用者の固有情報が記憶されており、利用者の固有情報として、例えば利用者の暗証番号、署名、指紋、声紋、網膜パターン、顔写真などが挙げられる。

#### 【 0 1 3 3 】

ハッシュ演算手段 3 1 5 では、復号手段 3 1 1 によって復号化された乱数と、利用者固有情報記憶手段 3 1 4 に記憶された利用者の固有情報とからハッシュ演算を行って、ハッシュ演算データ H 2 が生成される。

#### 【 0 1 3 4 】

暗号化手段 3 1 6 A では、判定信号の結果が「有」の場合（返信要求 I D が含まれていたと判断された場合）には、ハッシュ演算手段 3 1 5 から供給されたハッシュ演算データ H 2 が、カード会社 I D 番号・秘密鍵記憶手段 3 1 0 から出力された秘密鍵 K s 1 に基づいて暗号化される。なお、判定信号の結果が「無」の場合（返信要求 I D が含まれていなかったと判断された場合）には、ハッシュ演算手段 3 1 5 から供給されたハッシュ演算データ H 2 は暗号化されず、処理を終了する。

#### 【 0 1 3 5 】

なお、本実施形態 2 におけるカードリーダー／カードライター 1 4 の構成については、実施形態 1 の場合と同様であるため、ここでは、その説明を省略する。

#### 【 0 1 3 6 】

図 8 は、本発明の実施形態 2 の本人認証システムを用いた本人認証処理手順を示すフローチャートである。

【0137】

まず、ステップ S 2 0 1 において、IC カード 1 2 A 側では、乱数発生手段 2 1 1 によって、乱数 D 1 をランダムに生成する。

【0138】

次に、ステップ S 2 0 2 では、暗号化手段 2 1 3 によって、生成された乱数 D 1 と返信要求 ID とを公開鍵 K p 1 に基づいて暗号化する。カード会社の ID 番号と、公開鍵 K p 1 に基づいて暗号化された乱数 D 1 と、公開鍵 K p 1 に基づいて暗号化された返信要求 ID とを、カードリーダー/カードライター 1 4 を介して電子印鑑 1 6 A に送信する。

【0139】

さらに、ステップ S 2 0 3 において、電子印鑑 1 6 A 側では、受信されたカード会社の ID 番号から秘密鍵 K s を特定する。

【0140】

さらに、ステップ S 2 0 4 では、公開鍵 K p 1 に基づいて暗号化された乱数 D 1 と、公開鍵 K p 1 に基づいて暗号化された返信要求 ID とを、復号手段 3 1 1 によって、ステップ S 2 0 3 で特定された秘密鍵 K s 1 に基づいて復号する。これによって、復号化された返信要求 ID と、復号化された乱数 D 2 とが得られる。

【0141】

さらに、ステップ S 2 0 5 では、復号化された乱数 D 2 と利用者固有情報記憶手段 3 1 4 に記憶されている利用者の固有情報とを、ハッシュ演算手段 3 1 5 によってハッシュ演算して、ハッシュ演算データ H 2 を生成する。

【0142】

さらに、ステップ S 2 0 6 では、復号化された返信要求 ID と返信要求 ID 記憶手段 3 1 2 に記憶されている返信要求 ID とを比較して、返信要求 ID が含まれているか否かを判断する。送信要求 ID が含まれていない場合 (NO) には、ステップ S 2 0 7 に進み、処理を終了する。一方、送信要求 ID が含まれている

場合（ＹＥＳ）には、ステップＳ２０８の処理に進む。

【０１４３】

さらに、ステップＳ２０８では、ステップＳ２０５で得られたハッシュ演算データＨ２を、暗号化手段３１６Ａによって、ステップＳ２０３で特定された秘密鍵Ｋｓに基づいて暗号化する。暗号化されたハッシュ演算データ（ハッシュ演算データＨ２を暗号化したもの）をＩＣカード１２Ａに送信する。

【０１４４】

一方、ＩＣカード１２Ａ側では、ステップＳ２０９において、ステップＳ２０１で得られた乱数Ｄ１と利用者固有情報記憶手段２１８に記憶されている利用者の固有情報とを、ハッシュ演算手段２１９によってハッシュ演算して、ハッシュ演算データＨ１を生成する。

【０１４５】

次に、ステップＳ２１０では、ＩＣカード１２Ａ側で受信された、暗号化されたハッシュ演算データを、復号手段２１６Ａによって公開鍵Ｋｐ１に基づいて復号することによって、ハッシュ演算データＨ３を得る。

【０１４６】

さらに、ステップＳ２１１では、ステップＳ２０９で生成されたハッシュ演算データＨ１と、ステップＳ２１０で得られたハッシュ演算データＨ３との照合を行う。その照合結果が一致した場合（ＹＥＳ）には、ステップＳ２１２の処理に進み、本人であると認める。一方、その照合結果が不一致であれば（ＮＯ）、ステップＳ２１３の処理に進み、本人として認めないという判断を下す。

【０１４７】

以上の暗号化技術中では、廃棄鍵の管理も重要であり、本実施形態２のように、利用者固有情報を導入することによって、鍵の廃棄頻度を軽減することができる。例えば、電子印鑑１６Ａが紛失した場合に、新たに発行される電子印鑑１６Ａに対して、同一鍵によって電子印鑑１６Ａを構成することができる。この場合、利用者固有情報記憶手段２１８に登録される利用者固有情報を変更するだけで、安全性を保つことができる。また、例えば、家族会員のように複数の利用者に対して同じ鍵を適用しても、利用者固有情報で利用者を特定することができるた

め、鍵の数を減らすことができる。登録された利用者固有情報は電子化データ（デジタルデータ）であり、例えば声紋などのように物理的に同じ情報であっても、デジタルデータとして登録された場合には毎回異なる情報となるため、利用者固有情報が不足することはない。

## 【 0 1 4 8 】

また、本実施形態 2 において、本人認証は IC カード 1 2 A と電子印鑑 1 6 A との間で行われているが、電子印鑑 1 6 A を用いて窓口などで本人認証を行う場合には、上記 IC カード 1 2 A の代りに認証用パーソナルコンピュータを用いることができる。本人であると確認された場合には、パーソナルコンピュータのディスプレイに利用者固有情報を表示することによって、その利用者固有情報を用いて、パーソナルコンピュータの操作者が目視で本人であることを確認することができる。

## 【 0 1 4 9 】

上記実施形態 1，2 で説明したように、本発明の電子印鑑 1 6，1 6 A を用いることによって、本人認証の安全性を大幅に向上させることができる。

## 【 0 1 5 0 】

例えば、公開鍵方式暗号技術に用いられる公開鍵と秘密鍵とを作成し、本人認証を必要とするカード会社、電子商取引を行う事業者など、関連部門に公開鍵を公開して、秘密鍵を電子印鑑 1 6，1 6 A に閉じ込めて希望者に配布することによって、本発明の電子印鑑 1 6，1 6 A を用いた本人認証を実現することができる。この電子印鑑 1 6，1 6 A は、実印と同様に利用することが可能である。

## 【 0 1 5 1 】

図 9 は、本発明の電子印鑑を応用可能な分野を示す図である。括弧の中は、従来の本人認証方法を示している。

## 【 0 1 5 2 】

従来では、例えば、カードによる買い物を行う場合などには、署名を目視確認することにより本人認証が行われている。また、カードによる現金引き出し、携帯電話などによる遠隔家電制御、カードによる携帯電話などの課金、パーソナルコンピュータへのアクセス、電子錠の開錠を行う場合などには、暗証番号を入力

することにより本人認証が行われている。また、入退室管理、給油・高速料の支払い、電車の乗車料金・公衆電話料金の支払いを行う場合などには、カードを確認することによって本人認証が行われており、カードの所持者は真性な利用者であると判断されている。また、車両防犯のためには、車両の鍵によって本人認証が行われており、鍵の保持者は車両の真性な利用者であると判断されている。また、市役所の窓口などでは、伝統印鑑により本人認証が行われており、書き留め郵便配達の受け取りでは、伝統印鑑またはサインにより本人認証が行われている。また、高級家電の盗難防止については、個人が管理しているだけであり、本人認証による使用許可などは行われていない。

## 【 0 1 5 3 】

このような分野で、本発明の電子印鑑 1 6, 1 6 A を従来の認証方法と組み合わせることで、利用者に負担をかけずに、安全性を格段に向上させることができる。暗証番号は、盗難にあっても被害が発生しない限り発覚されないが、本発明の電子印鑑 1 6, 1 6 A は盗難にあったときに気が付き易く、被害防止対策を早急に行うことができる。また、電子印鑑 1 6, 1 6 A を紛失しただけでは、被害は生じにくい。

## 【 0 1 5 4 】

従来は、市役所の窓口などでの本人認証、書き留め郵便配達の受け取りには、伝統印鑑が用いられているが、今後、例えば国民総背番号制などのように、個人情報電子データ化され、そのデータを利用して情報・サービスが提供されると共に個人の権利・義務が管理されるような、いわゆる電子化政府になっていくことを考えると、本発明の電子印鑑 1 6, 1 6 A を伝統印鑑に変えて利用することは、非常に有効である。

## 【 0 1 5 5 】

また、高級家電製品などに本人認証機能を加えることによって、盗難を防止することができる。テレビジョンセット、冷蔵庫、ビデオ、カメラなどの電子機器に対して、本発明の電子印鑑 1 6, 1 6 A による本人認証機能を設けて、電源投入の際に本人認証を要求することによって、本発明の電子印鑑 1 6, 1 6 A が無いと、これらの電子機器が作動しないことになる。このような機能は、発展途上

国において実効性がある。

【 0 1 5 6 】

さらに、定期券などの I C カードにおいて、本発明の電子印鑑 1 6, 1 6 A に  
よる本人認証機能を設けることによって、I C カードを紛失した場合の届率が高  
くなると考えられる。

【 0 1 5 7 】

【発明の効果】

以上説明したように、本発明によれば、秘密鍵に基づいて暗号化・復号化を行  
う電子印鑑を導入することによって、利用者に負担をかけることなく、本人認証  
の安全性を大幅に向上させることができる。

【 0 1 5 8 】

また、利用者の署名、指紋、声紋、網膜パターン、顔写真など、利用者固有の  
情報を電子データ化して、暗号化技術を用いてデータを送受信して確認すること  
より、本人認証の安全性をより向上させることができる。

【 0 1 5 9 】

さらに、電子印鑑は、指輪、ブレスレット、イヤリングなどのアクセサリ、  
眼鏡など、利用者が身に付けてあまり離さないような携帯機器に装着することに  
よって、紛失しにくくすることができ、さらに安全性を向上させることができる  
。また、電子印鑑は、盗難などに遭った場合に気付きやすいため、無形の暗証番  
号に比べて被害防止対策を早急に行うことができる。

【図面の簡単な説明】

【図 1】

本発明の本人認証システムの実施形態 1 における要部構成を示すブロック図で  
ある。

【図 2】

図 1 の I C カードの内部構成を示すブロック図である。

【図 3】

図 1 の電子印鑑 1 6 の内部構成を示すブロック図である。

【図 4】

図 1 のカードリーダー／カードライタの内部構成を示すブロック図である。

【図 5】

図 1 の本人認証システムを用いた本人認証処理手順を示すフローチャートである。

【図 6】

本発明の本人認証システムの実施形態 2 における I C カードの内部構成を示すブロック図である。

【図 7】

本発明の本人認証システムの実施形態 2 における電子印鑑の内部構成を示すブロック図である。

【図 8】

本発明の実施形態 2 における本人認証システムを用いた本人認証処理手順を示すフローチャートである。

【図 9】

本発明の電子印鑑を応用可能な分野を示す図である。

【図 1 0】

従来の本人認証システムの一例を示すブロック図である。

【符号の説明】

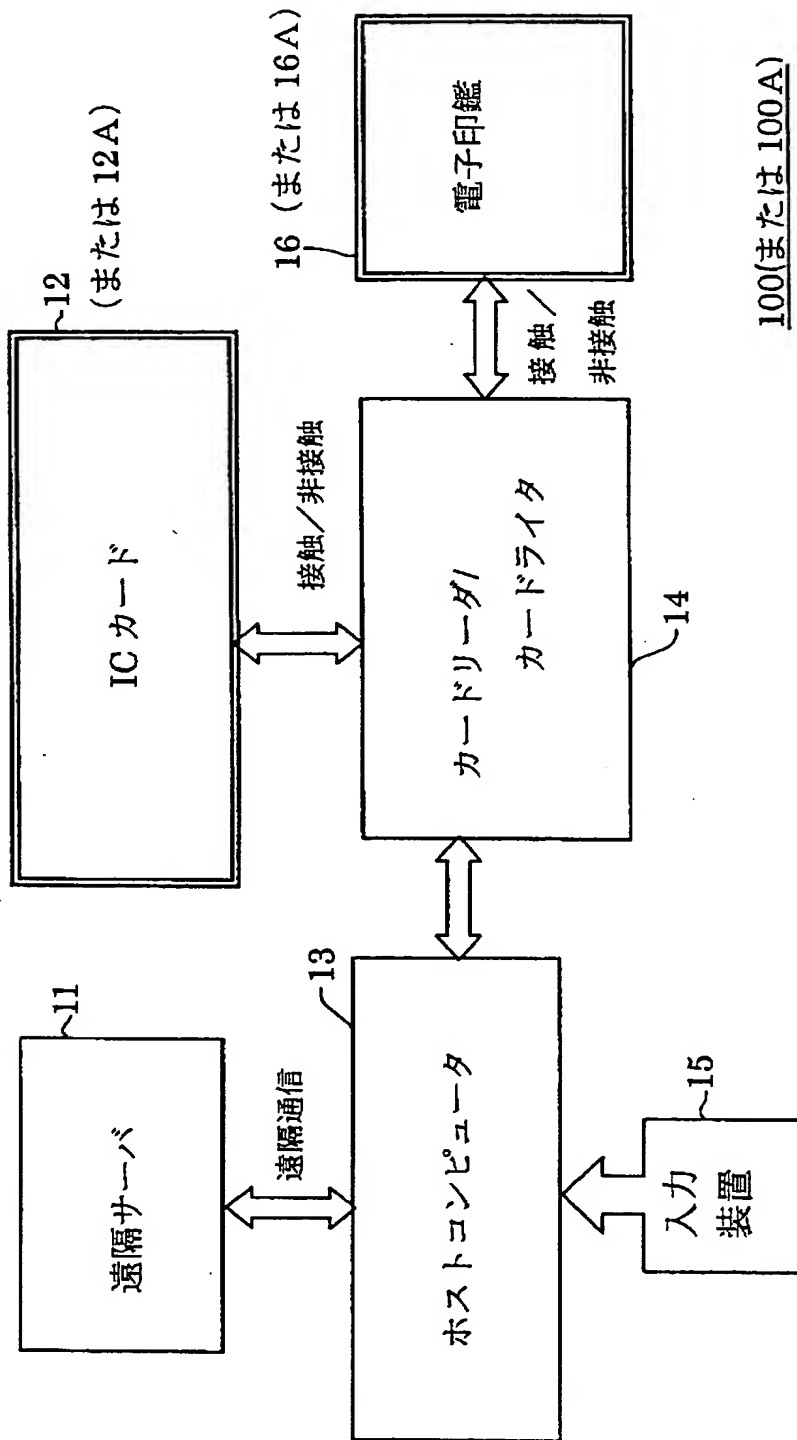
- 1 1      遠隔サーバ
- 1 2, 1 2 A      I C カード
- 1 3      ホストコンピュータ
- 1 4      カードリーダー／カードライタ
- 1 5      入力装置
- 1 6, 1 6 A      電子印鑑
- 1 0 0, 1 0 0 A      本人認証システム
- 2 0 1, 3 0 1, 4 0 3      アンテナ回路
- 2 0 2, 3 0 2      整流回路
- 2 0 3, 3 0 3      クロック抽出回路
- 2 0 4, 3 0 4      復調回路



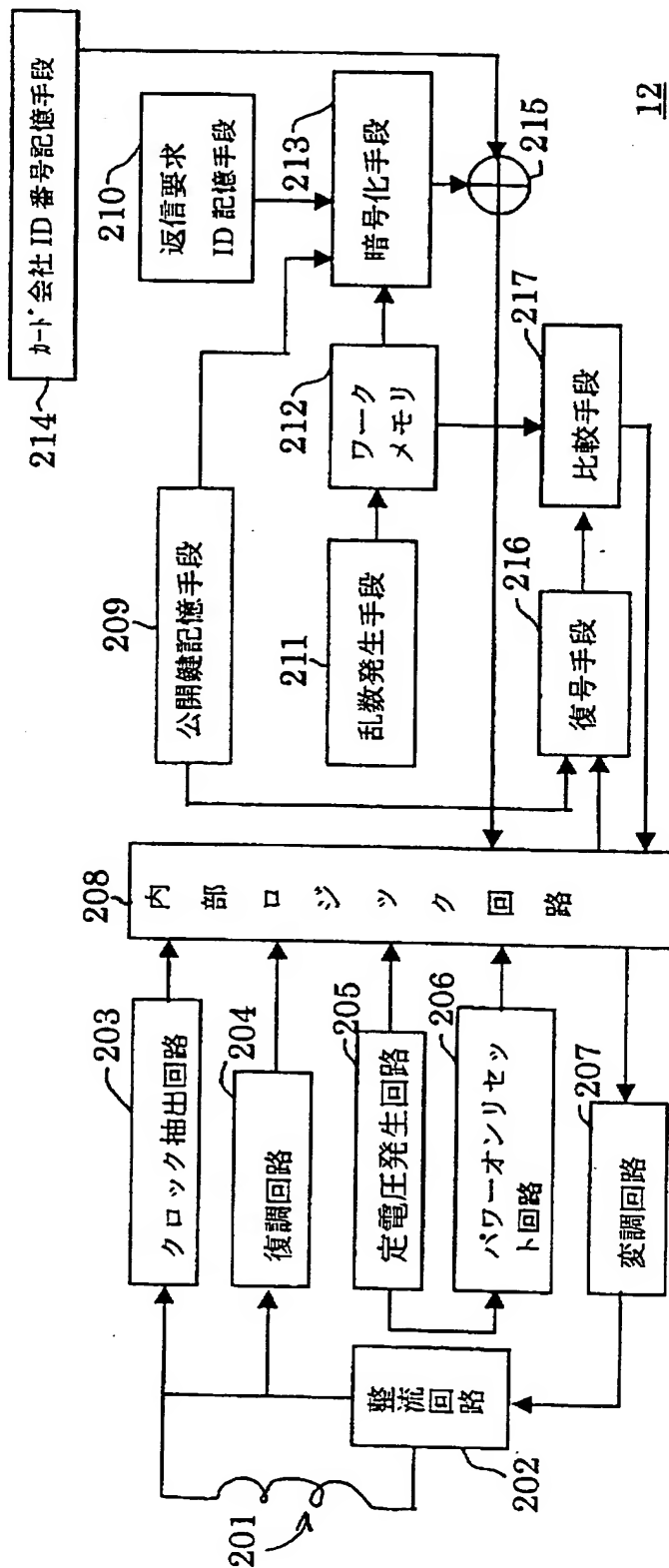
- 2 0 5, 3 0 5      定電圧発生回路
- 2 0 6, 3 0 6      パワーオンリセット回路
- 2 0 7, 3 0 7      変調回路
- 2 0 8, 3 0 8      内部ロジック回路
- 2 0 9      公開鍵記憶手段
- 2 1 0, 3 1 2      返信要求 I D 記憶手段
- 2 1 1      乱数発生手段
- 2 1 2      ワークメモリ
- 2 1 3, 3 1 4, 3 1 6 A      暗号化手段
- 2 1 4      カード会社 I D 番号記憶手段
- 2 1 5      合成回路
- 2 1 6, 2 1 6 A, 3 1 1      復号手段
- 2 1 7, 2 1 7 A      比較手段
- 2 1 8      利用者固有情報記憶手段
- 2 1 9, 3 1 5      ハッシュ演算手段
- 3 0 9      分離手段
- 3 1 0      カード会社 I D 番号・秘密鍵記憶手段
- 3 1 3      返信要求 I D 有無判断手段
- 3 1 4      利用者固有情報記憶手段
- 4 0 1      変調回路
- 4 0 2      復調回路
- 4 0 4      不揮発性メモリ
- 4 0 5      信号処理回路
- 4 0 6      制御回路
- 4 0 7      入出力 I / F

【書類名】 図面

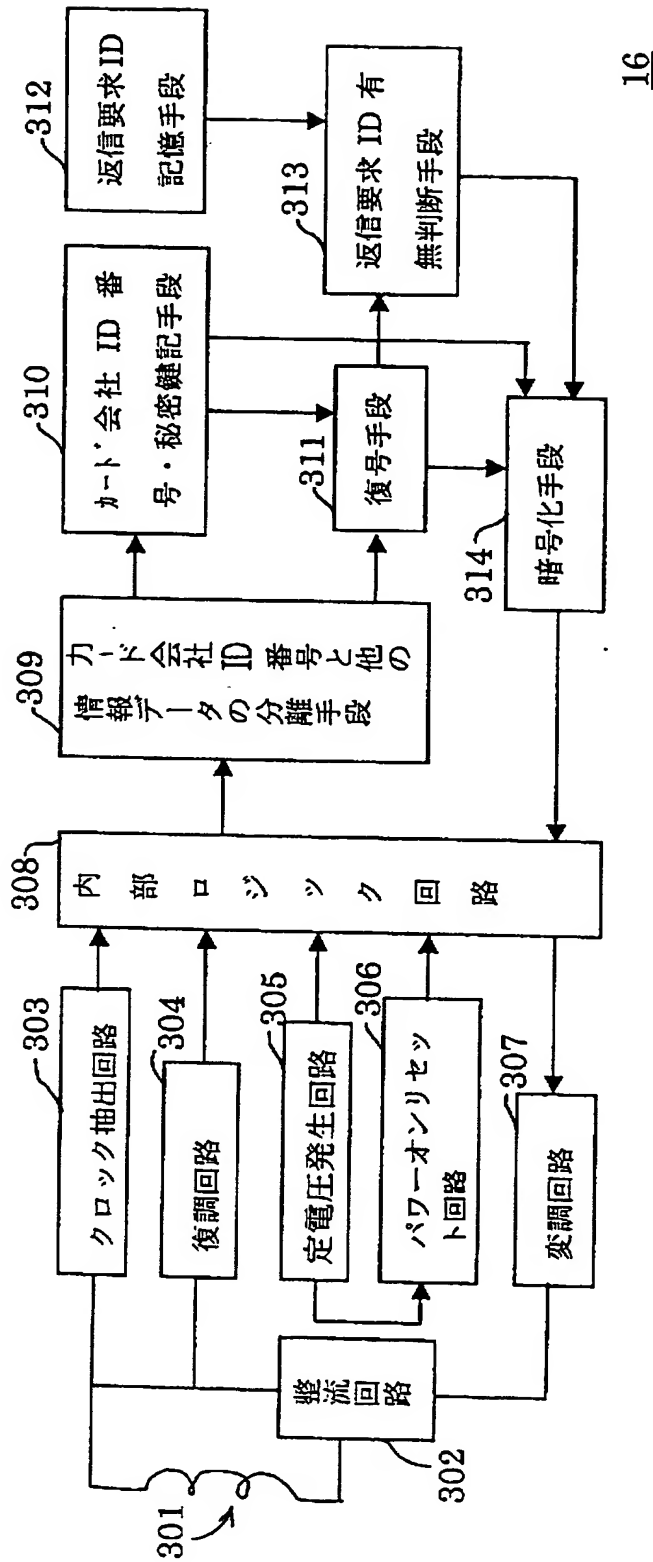
【図 1】



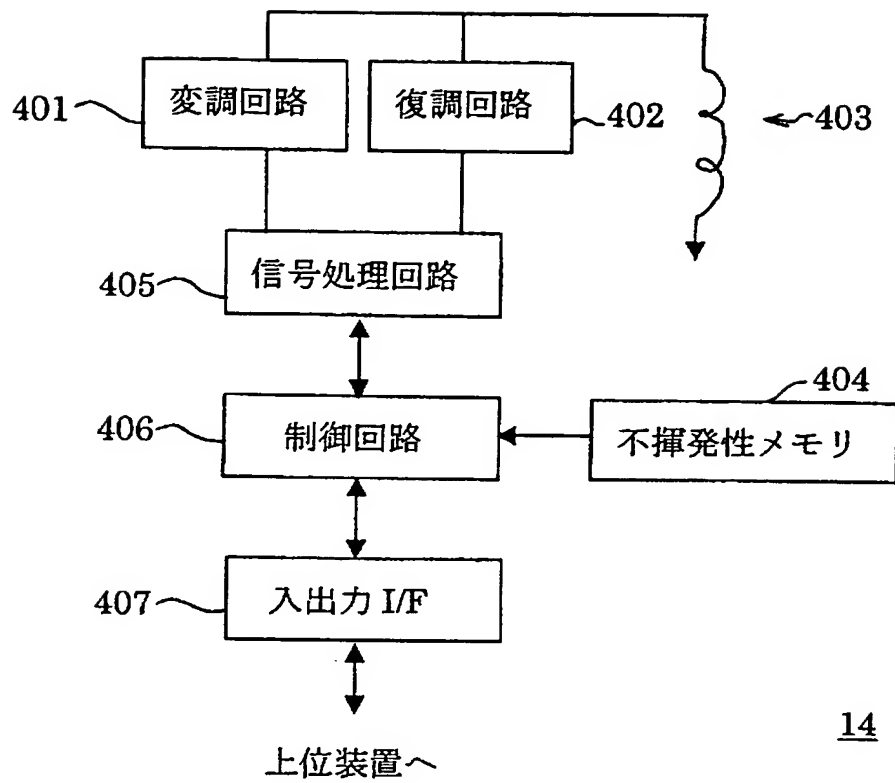
【図 2】



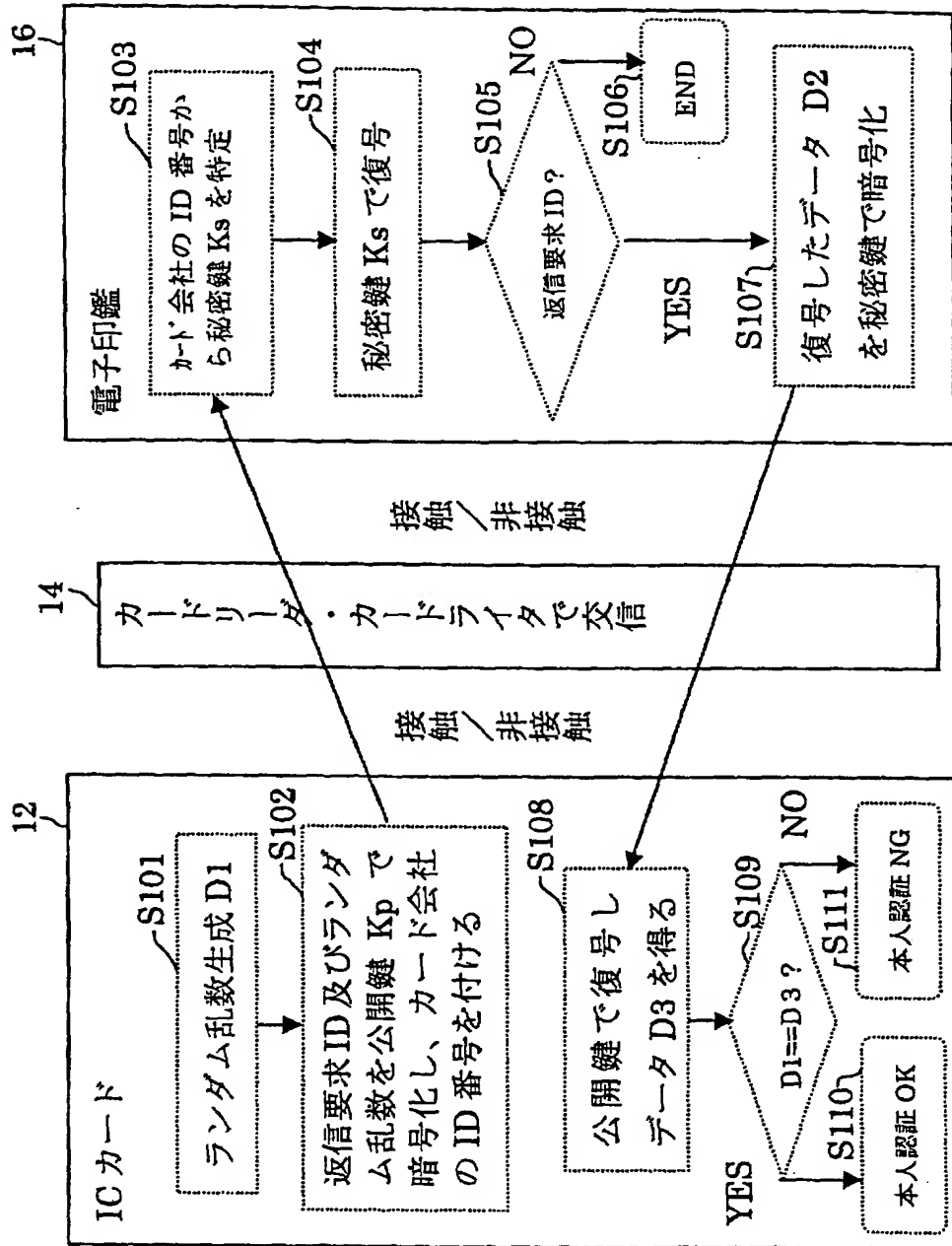
【図 3】



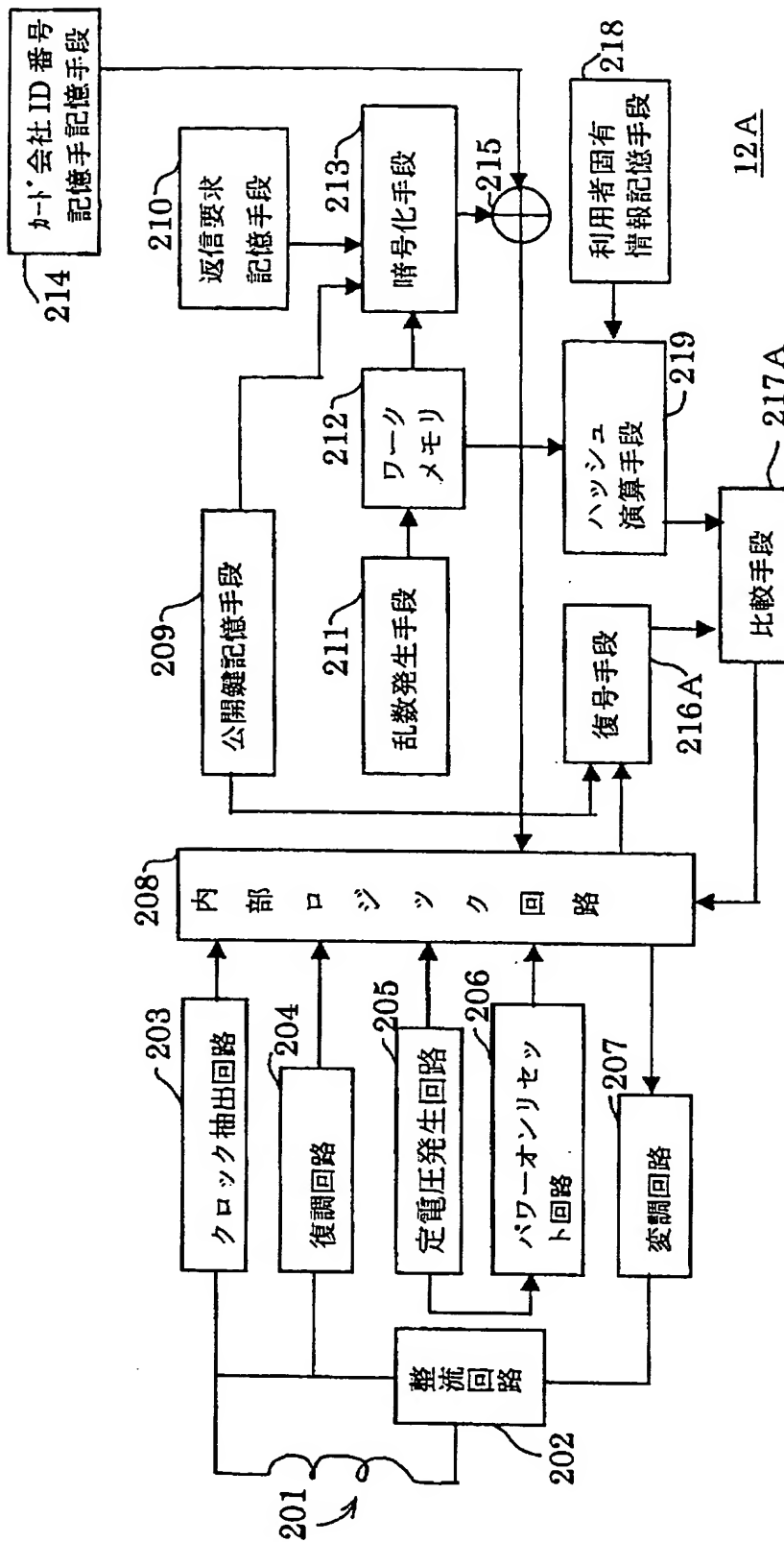
【図 4】



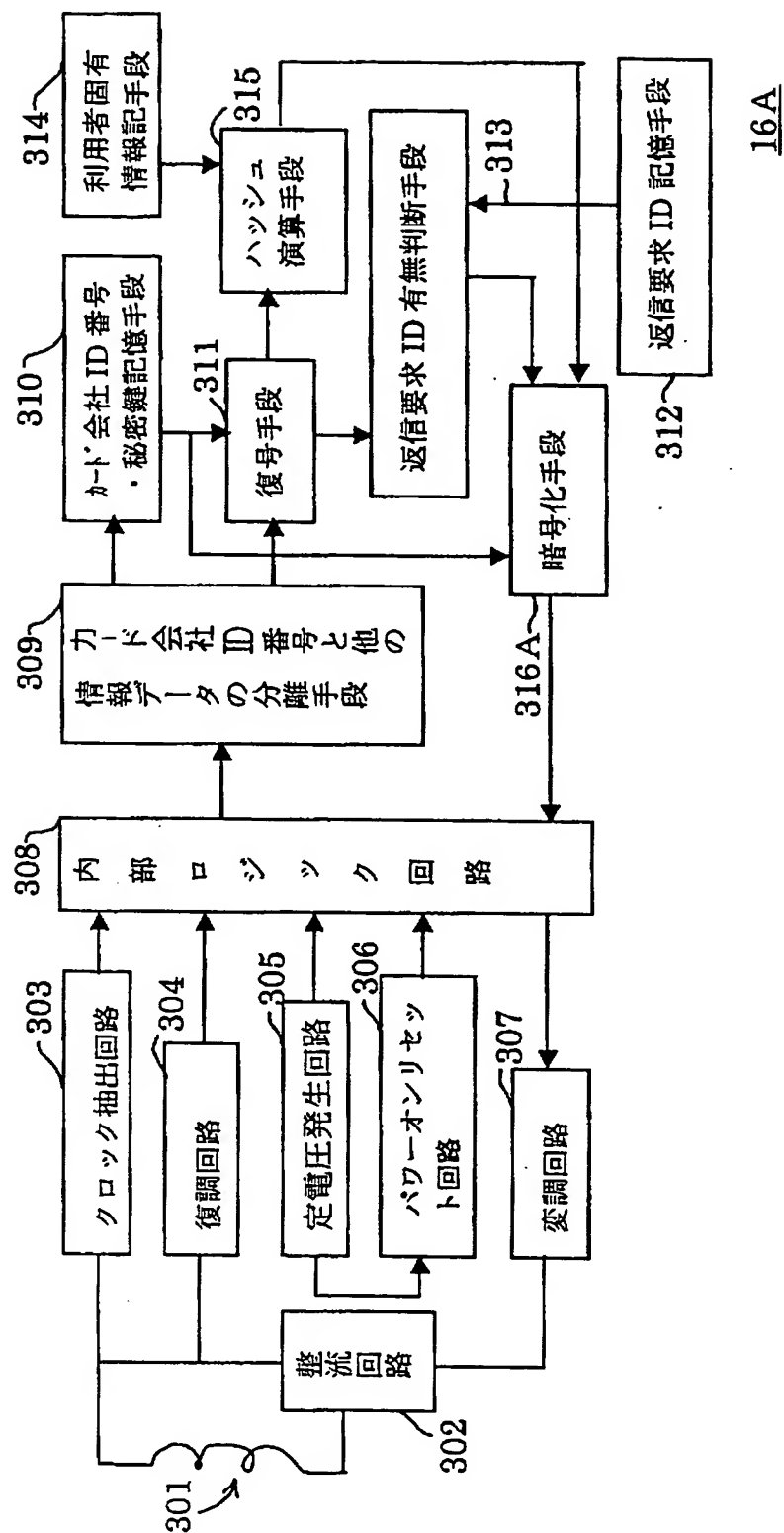
【図5】



【図 6】



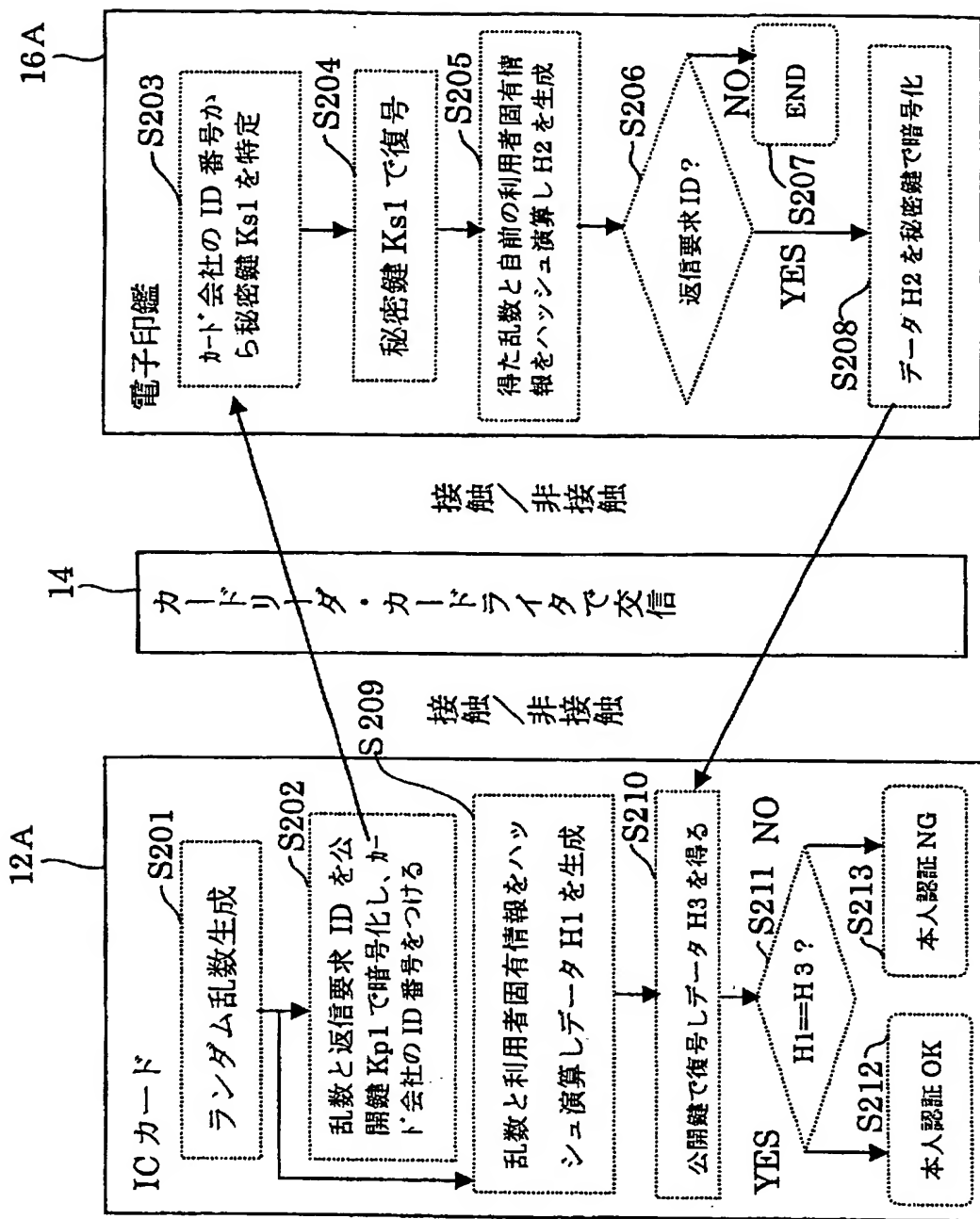
【図 7】



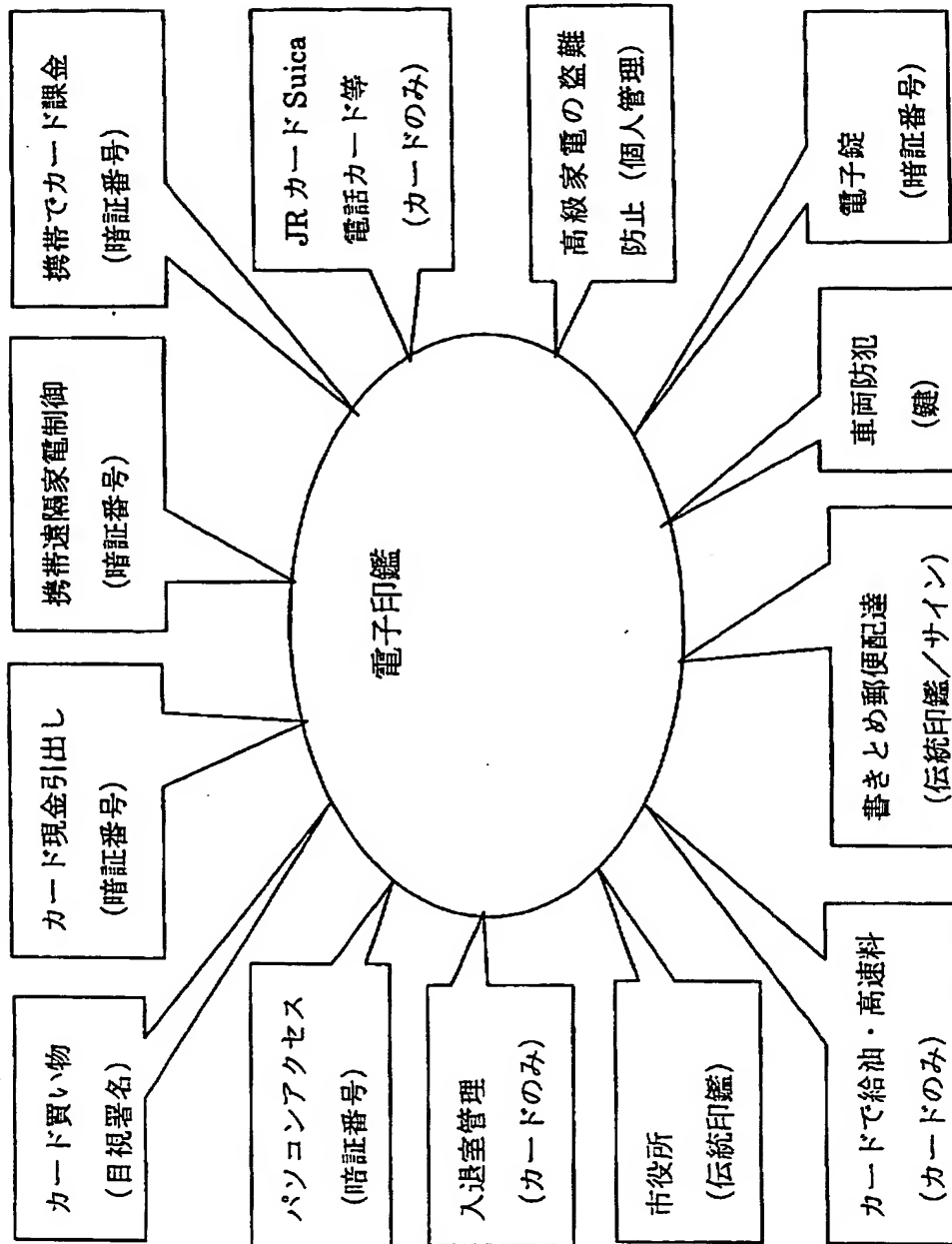
16A



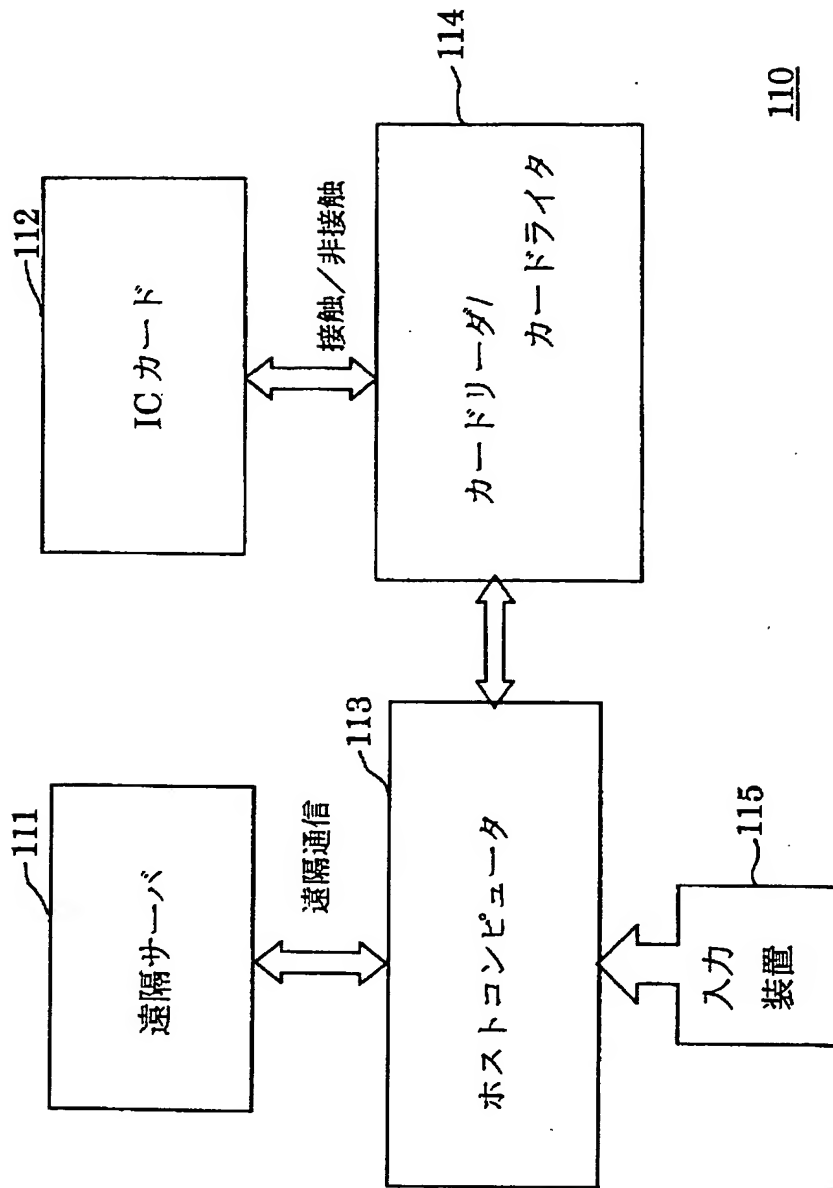
【図 8】



【図9】



【図10】



【書類名】 要約書

【要約】

【課題】 利用者に負担をかけることなく、本人認証の安全性を高める。

【解決手段】 公開鍵に基づいて暗号化・復号化を行う IC カード 1 2 と、秘密鍵に基づいて暗号化・復号化を行う電子印鑑 1 6 とを組み合わせる公開鍵方式暗号技術により本人認証を行う。まず、IC カード 1 2 によって乱数値を生成し、乱数値と返信要求 ID とを公開鍵に基づいて暗号化して電子印鑑 1 6 に送信する。電子印鑑 1 6 では、受信された信号を秘密鍵に基づいて復号化し、返信要求 ID が含まれている場合には、復号化された乱数値を秘密鍵に基づいて暗号化して IC カード 1 2 に送信する。IC カード 1 2 では、受信された乱数値を公開鍵に基づいて復号化し、復号化された乱数値と元の乱数値とが一致した場合に、本人であると確認する。

【選択図】 図 5

認定・付加情報

特許出願の番号	特願2002-225590
受付番号	50201145534
書類名	特許願
担当官	第七担当上席 0096
作成日	平成14年 8月 5日

<認定情報・付加情報>

【特許出願人】

【識別番号】 000005049

【住所又は居所】 大阪府大阪市阿倍野区長池町22番22号

【氏名又は名称】 シャープ株式会社

【代理人】 申請人

【識別番号】 100078282

【住所又は居所】 大阪市中央区城見1丁目2番27号 クリスタル  
タワー15階

【氏名又は名称】 山本 秀策

【選任した代理人】

【識別番号】 100062409

【住所又は居所】 大阪府大阪市中央区城見1丁目2番27号 クリ  
スタルタワー15階 山本秀策特許事務所

【氏名又は名称】 安村 高明

【選任した代理人】

【識別番号】 100107489

【住所又は居所】 大阪市中央区城見一丁目2番27号 クリスタル  
タワー15階 山本秀策特許事務所

【氏名又は名称】 大塩 竹志

出 願 人 履 歴 情 報

識別番号 [000005049]

1. 変更年月日 1990年 8月29日

[変更理由] 新規登録

住 所 大阪府大阪市阿倍野区長池町22番22号

氏 名 シャープ株式会社